



Federal Register

**Thursday,
January 25, 2007**

Part II

Department of Homeland Security

Coast Guard

**33 CFR Parts 1, 20 et al. and 46 CFR
Parts 1, 4 et al.**

Transportation Security Administration

**49 CFR Parts 10, 12, and 15
Transportation Worker Identification
Credential (TWIC) Implementation in the
Maritime Sector; Final Rule
Consolidation of Merchant Mariner
Qualification Credentials; Proposed Rule**

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Parts 101, 103, 104, 105, 106, 125 and 46 CFR Parts 10, 12, 15
Transportation Security Administration
49 CFR Parts 1515, 1540, 1570, 1572
[Docket Nos. TSA-2006-24191; Coast Guard-2006-24196; TSA Amendment Nos. 1515-(New), 1540-8, 1570-2, 1572-7]

RIN 1652-AA41

Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License

AGENCY: Transportation Security Administration; United States Coast Guard, DHS.

ACTION: Final rule; request for comments.

SUMMARY: The Department of Homeland Security (DHS), through the Transportation Security Administration (TSA) and the United States Coast Guard (Coast Guard), issues this final rule to further secure our Nation's ports and modes of transportation. This rule implements the Maritime Transportation Security Act of 2002 and the Security and Accountability for Every Port Act of 2006. Those statutes establish requirements regarding the promulgation of regulations that require credentialed merchant mariners and workers with unescorted access to secure areas of vessels and facilities to undergo a security threat assessment and receive a biometric credential, known as a Transportation Worker Identification Credential (TWIC). After DHS publishes a notice announcing the compliance date for each Captain of the Port (COTP) zone, persons without TWICs will not be granted unescorted access to secure areas at affected maritime facilities. Those seeking unescorted access to secure areas aboard affected vessels, and all Coast Guard credentialed merchant mariners must possess a TWIC by September 25, 2008. This final rule will enhance the security of ports by requiring such security threat assessments of persons in secure areas and by improving access control measures to prevent those who may pose a security threat from gaining unescorted access to secure areas of ports.

With this final rule, the Coast Guard amends its regulations on vessel and facility security to require the use of the TWIC as an access control measure. The

Coast Guard also amends its merchant mariner regulations to incorporate the requirement to obtain a TWIC. This final rule does not include the card reader requirements for owners and operators set forth in the Notice of Proposed Rulemaking (NPRM) issued in this matter on May 22, 2006. Such requirements will be addressed in a future rulemaking. Although the card reader requirements are not being implemented at this time, the Coast Guard will institute periodic unannounced checks to confirm the identity of the holder of the TWIC.

With this final rule, TSA applies its security threat assessment standards that currently apply to commercial drivers authorized to transport hazardous materials in commerce to merchant mariners and workers who require unescorted access to secure areas on vessels and at maritime facilities. This final rule amends TSA regulations in a number of ways. To minimize redundant background checks of workers, TSA amends the threat assessment standards to include a process by which TSA determines if a security threat assessment conducted by another governmental agency or by TSA for another program is comparable to the standards in this rule. TSA amends the qualification standards by changing the list of crimes that disqualify an individual from holding a TWIC or a hazardous materials endorsement.

TSA expands the appeal and waiver provisions to apply to TWIC applicants and air cargo employees who undergo a security threat assessment. These modifications include a process for the review of adverse waiver decisions and certain disqualification cases by an administrative law judge (ALJ). TSA also extends the time period in which applicants may apply for an appeal or waiver.

Finally, this rule establishes the user fee for the TWIC and invites comment on one component of the fee, the card replacement fee.

Under this rule, TSA will begin issuing first generation TWIC cards at initial port deployment locations. These TWIC cards will not initially support contactless biometric operations, but the TWIC cards will be functional with certain existing access control systems in use at ports today.

TSA and the Coast Guard have established a working group, comprised of members of the maritime and technology industries, through the National Maritime Security Advisory Committee (NMSAC), a federal advisory committee to the Coast Guard. This working group, in consultation with the National Institute for Standards and

Technology (NIST), is tasked with recommending the contactless biometric software specification for TWIC cards.

TSA will publish a notice detailing the draft contactless biometric software specification for TWIC cards no later than the date by which it publishes the final TWIC fee as required by this Rule. Currently those notices are expected to be published in February 2007. TSA will subsequently publish a final specification for TWIC contactless biometric software functionality and the associated specifications for TWIC card readers. TSA plans also to write electronically the contactless biometric software application to all issued TWIC cards after publication of this specification. After initial field testing, this additional contactless biometric function will be included with all TWIC cards produced after publication of the contactless biometric software specification.

Although this rule goes into effect on March 26, 2007, the requirements to hold a TWIC, and to restrict access to secure areas of a facility or OCS facility, will be effective only after the regulated party is notified by DHS. These notifications will be published in the **Federal Register** and will require compliance on a COTP by COTP basis. Those seeking unescorted access to secure areas aboard affected vessels, and all Coast Guard credentialed merchant mariners must possess a TWIC by September 25, 2008.

DATES: *Effective Date:* This rule is effective March 26, 2007.

Comment Date: Comments with respect to the Card Replacement Fee must be submitted by February 26, 2007.

ADDRESSES: Comments and material received from the public, as well as documents mentioned in this preamble as being available in the docket, are part of dockets TSA-2006-24191 and Coast Guard-2006-24196 and are available for inspection or copying at the Docket Management Facility, U.S. Department of Transportation, room PL-401, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet at <http://dms.dot.gov>.

You may submit comments identified by docket number TSA-2006-24191 to the Docket Management Facility at the U.S. Department of Transportation. To avoid duplication, please use only one of the following methods:

(1) *Web Site:* <http://dms.dot.gov>.

(2) *Mail:* Docket Management Facility, U.S. Department of Transportation, 400

Seventh Street SW., Room PL-401, Washington, DC 20590-0001.

(3) Fax: 202-493-2251.

(4) *Delivery*: Room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.

(5) *Federal eRulemaking Portal*: <http://www.regulations.gov>.

See **SUPPLEMENTARY INFORMATION** for format and other information about comment submissions.

FOR FURTHER INFORMATION CONTACT: For questions related to TSA's standards: Greg Fisher, Transportation Security Administration, TSA-19, 601 South 12th Street, Arlington, VA 22202-4220, TWIC Program, (571) 227-4545; e-mail: credentialing@dhs.gov.

For legal questions: Christine Beyer, TSA-2, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220; telephone (571) 227-2657; facsimile (571) 227-1380; e-mail Christine.Beyer@dhs.gov.

For questions concerning the Coast Guard provisions of the TWIC rule: LCDR Jonathan Maiorine, Commandant (G-PCP-2), United States Coast Guard, 2100 Second Street, SW., Washington, DC 20593; telephone 1-877-687-2243.

For questions concerning viewing or submitting material to the docket: Renee V. Wright, Program Manager, Docket Management System, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street, SW., Washington, DC 20590-0001; telephone (202) 493-0402.

SUPPLEMENTARY INFORMATION:

Comments Invited

TSA invites comment on one provision of the rule, the Card Replacement Fee, as discussed in section I under Fees and section VI of this preamble. See **ADDRESSES** above for information on where to submit comments. With each comment, please include your name and address, identify the docket number at the beginning of your comments, and give the reason for each comment. Please explain the reason for any recommended change and include supporting data. You may submit comments and material electronically, in person, by mail, or fax as provided under **ADDRESSES**, but please submit your comments and material by only one means. If you submit comments by mail or delivery, submit them in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

If you want TSA to acknowledge receipt of comments submitted by mail,

include with your comments a self-addressed, stamped postcard on which the docket number appears. We will stamp the date on the postcard and mail it to you.

TSA will file in the public docket all comments received by TSA, except for comments containing confidential information and sensitive security information (SSI)¹. TSA will consider all comments received on or before the closing date for comments and will consider comments filed late to the extent practicable. The docket is available for public inspection before and after the comment closing date.

Handling of Confidential or Proprietary Information and Sensitive Security Information (SSI) Submitted in Public Comments

Do not submit comments that include trade secrets, confidential commercial or financial information, or SSI to the public regulatory docket. Please submit such comments separately from other comments on the rulemaking. Comments containing this type of information should be appropriately marked as containing such information and submitted by mail to the address listed in the **FOR FURTHER INFORMATION CONTACT** section. Upon receipt of such comments, TSA will not place the comments in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. TSA will hold them in a separate file to which the public does not have access, and place a note in the public docket that TSA has received such materials from the commenter. If TSA receives a request to examine or copy this information, TSA will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Department of Homeland Security's (DHS's) FOIA regulation found in 6 CFR part 5.

Reviewing Comments in the Docket

Please be aware that anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the applicable Privacy Act Statement published in the **Federal Register** on April 11, 2000 (65 FR

19477), or you may visit <http://dms.dot.gov>.

You may review the comments in the public docket by visiting the Dockets Office between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The Dockets Office is located on the plaza level of the Nassif Building at the Department of Transportation address, previously provided under **ADDRESSES**. Also, you may review public dockets on the Internet at <http://dms.dot.gov>.

Availability of Rulemaking Document

You can get an electronic copy of this document as well as other documents associated with this rulemaking on the Internet by—

(1) Searching the Department of Transportation's electronic Docket Management System (DMS) web page (<http://dms.dot.gov/search>);

(2) Accessing the Government Printing Office's web page at <http://www.gpoaccess.gov/fr/index.html>; or

(3) Visiting TSA's Security Regulations web page at <http://www.tsa.gov> and accessing the link for "Research Center" at the top of the page.

Abbreviations and Terms Used in This Document

ALJ—Administrative Law Judge
 AMS—Area Maritime Security
 ASP—Alternative Security Program
 CBP—Bureau of Customs and Border Protection
 CDC—Certain Dangerous Cargo
 CDL—Commercial drivers license
 CDLIS—Commercial drivers license information system
 CHRC—Criminal history records check
 CJIS—Criminal Justice Information Services Division
 COR—Certificate of Registry
 COTP—Captain of the Port
 DHS—Department of Homeland Security
 DOJ—Department of Justice
 DOT—Department of Transportation
 FBI—Federal Bureau of Investigation
 FMCSA—Federal Motor Carrier Safety Administration
 FMSC—Federal Maritime Security Coordinator
 FSP—Facility Security Plan
 HME—Hazardous materials endorsement
 HSA—Homeland Security Act
 HSPD 12—Homeland Security Presidential Directive 12
 MARSEC—Maritime Security
 MMD—Merchant Mariner's Document
 MSC—Marine Safety Center
 MTSA—Maritime Transportation Security Act
 NIST—National Institute of Standards and Technology

¹ "Sensitive Security Information" or "SSI" is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

NPRM—Notice of Proposed Rulemaking
 NVIC—Navigation and Vessel
 Inspection Circular
 OCS—Outer Continental Shelf
 REC—Regional Examination Center
 SAFETEA—LU—Safe, Accountable,
 Flexible, Efficient Transportation
 Equity Act—A Legacy for Users
 STCW—International Convention on
 Standards of Training, Certification,
 and Watchkeeping for Seafarers, 1978,
 as amended
 TSA—Transportation Security
 Administration
 TPS—Temporary Protected Status
 TWIC—Transportation Worker
 Identification Credential
 VSP—Vessel Security Plan

Table of Contents

- I. Background
- II. Final Rule
 - A. Coast Guard Provisions
 - B. TSA Provisions
 - C. Changes From NPRM
 - D. Anticipated Future Notices and Rulemaking
 - E. Summary of TWIC Process under the Final Rule
 - F. SAFE Port Act of 2006
- III. Discussion of Comments
 - A. Requests for Extension of Comment Period and Additional Public Meetings
 - B. Coast Guard Provisions
 - 1. Definitions
 - 2. General Comments on Applicability
 - 3. Coast Guard Roles
 - 4. Owner/operator Requirements
 - 5. Requirements for Security Officers and Personnel
 - 6. Recordkeeping/Tracking Persons on Vessels/Security Incident Procedures
 - 7. Reader Requirements/Biometric Verification/TWIC Validation Procedures
 - 8. Access Control Issues
 - 9. TWIC Addendum
 - 10. Compliance Dates
 - 11. General Compliance Issues
 - 12. Additional Requirements—Cruise Ships
 - 13. Additional Requirements—Cruise Ship Terminals
 - 14. Additional Requirements—CDC Facilities
 - 15. Additional Requirements—Barge Fleeting Facilities
 - 16. Miscellaneous
 - C. TSA Provisions
 - 1. Technology Concerns
 - 2. Enrollment Issues
 - 3. Appeal and Waiver Issues
 - 4. TSA Inspection
 - 5. Security Threat Assessment
 - 6. Immigration Status
 - 7. Mental Incapacity
 - 8. TWIC Expiration and Renewal Periods
 - 9. Fees for TWIC
 - 10. Implementing TWIC in Other Modes
 - D. Comments Relating to Economic Issues
 - E. Comments Beyond the Scope of the Rule
- IV. Advisory Committee Recommendations and Responses
- V. Rulemaking Analyses and Notices
 - A. Regulatory Planning and Review (Executive Order 12866)

- B. Small Entities
- C. Assistance for Small Entities
- D. Collection of Information
- E. Federalism (Executive Order 13132)
- F. Unfunded Mandates Reform Act
- G. Taking of Private Property
- H. Civil Justice Reform
- I. Protection of Children
- J. Indian Tribal Governments
- K. Energy Effects
- L. Technical Standards
- M. Environment
- VI. Solicitation of Comments

I. Background

The Department of Homeland Security (DHS), through the United States Coast Guard (Coast Guard) and the Transportation Security Administration (TSA), issues this final rule pursuant to the Maritime Transportation Security Act (MTSA), Pub. L. 107–295, 116 Stat. 2064 (November 25, 2002), and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), Pub. L. 109–347 (October 13, 2006). Section 102 of MTSA (46 U.S.C. 70105) requires DHS to issue regulations to prevent individuals from entering secure areas of vessels or MTSA-regulated port facilities unless such individuals hold transportation security cards issued under section 102 and are authorized to be in the secure areas. An individual who does not hold the required transportation security card, but who is otherwise authorized to be in the secure area in accordance with the facility's security plan, must be accompanied by another individual who holds a transportation security card. MTSA also requires all credentialed merchant mariners to hold these transportation security cards, and requires DHS to establish a waiver and appeals process for persons found to be ineligible for the required transportation security card. The SAFE Port Act contained amendments to the basic MTSA requirements for credentialing (concurrent processing, fees, card readers, program roll out, testing and timelines) as well as added new requirements (disqualifying crimes, new hire provisions and discretion as to who may obtain a TWIC). The substance of the SAFE Port Act is discussed in greater detail later in this document.

On May 22, 2006, TSA and the Coast Guard issued a joint notice of proposed rulemaking (71 FR 29396), setting forth the proposed requirements and processes required under sec. 102 of MTSA (TWIC NPRM) for implementation of the TWIC program in the maritime sector. The NPRM proposed changes to three titles of TSA and Coast Guard regulations (33 CFR, 46 CFR, and 49 CFR). The Department

intends for these combined changes to increase port security by requiring all credentialed mariners and all persons who require unescorted access to a regulated facility or vessel to have undergone a security threat assessment by TSA and obtain a TWIC.² The proposed security threat assessment included a review of criminal, immigration, and pertinent intelligence records. TSA also proposed a process for individuals denied TWICs to appeal adverse determinations or apply for waivers of the standards.

Prior to the publication of the TWIC NPRM, the Coast Guard published a Notice in the **Federal Register** informing the public that the Commandant of the Coast Guard, pursuant to his authority under 50 U.S.C. 191 and 33 CFR part 125, was exercising his authority to require identification credentials for persons seeking access to waterfront facilities and to port and harbor areas, including vessels and harbor craft in such areas. 71 FR 25066 (April 28, 2006). This action has served as an interim measure to improve security at our nation's ports by verifying maritime workers' identities, validating their background information, and accounting for access for authorized personnel to transportation facilities, vessels and activities. *Id.*

The May 22, 2006 TWIC NPRM provided the draft regulatory text for review and solicited public comments for 45 days. TSA and the Coast Guard also held four public meetings throughout the country to solicit public comments. Those meetings were held on May 31, 2006 in Newark, New Jersey; on June 1, 2006 in Tampa, Florida; on June 6, 2006 in St. Louis, Missouri; and on June 7, 2006 in Long Beach, California. Approximately 1200 people attended these meetings. The public can view transcripts of the four public meetings on the public docket for this rulemaking action at www.regulations.gov. DHS also received approximately 1770 written comments on the TWIC NPRM. Those comments also can be accessed through the public docket for this action. TSA and the Coast Guard respond to the comments received in the "Discussion of Comments" section, below.

Many commenters requested an extension of the comment period and additional public meetings. As explained more fully in the "Discussion of Comments" section below, DHS has decided not to delay implementation of the TWIC program by extending the

² Additional information on the statutory and regulatory history of this rule can be found in the NPRM at 71 FR 29396 (May 22, 2006).

comment period or providing additional public meetings because it is imperative to begin implementation of the TWIC requirements, and accompanying security threat assessments, as soon as possible to improve the security of our Nation's vessels and port facilities. TSA and Coast Guard, however, have not promulgated in this final rule the proposed requirements on owners and operators relating to biometric readers. The Department will address those proposed requirements, which generated the majority of the comments received on the NPRM, in a separate rulemaking action. Interested parties will have the opportunity to comment on those provisions during that rulemaking action. Although the card reader requirements are not being implemented under this final rule, Coast Guard personnel will periodically, and without advance notice, use handheld readers to check the biometric information contained in the card to confirm the identity of the holder of the TWIC.

On May 22, 2006, the Coast Guard also published a related proposed rule, "Consolidation of Merchant Mariner Qualification Credentials," at 71 FR 29462 (MMC NPRM), proposing the consolidation of Coast Guard-issued merchant mariner's document (MMD), merchant mariner's license (license), certificate of registry (COR) and International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW) certificate into a single credential called the merchant mariner credential (MMC). The MMC NPRM proposed to streamline the application process, and reduce the administrative burden for the public and the Federal Government. The public meetings held on the TWIC NPRM also included time for the Coast

Guard to receive comments on the MMC NPRM. In a separate rulemaking action published elsewhere in this edition of the **Federal Register**, the Coast Guard has provided a Supplemental Notice of Proposed Rulemaking (SNPRM) also entitled "Consolidation of Merchant Mariner Qualification Credentials." The purpose of the SNPRM is to address comments received from the public on the MMC NPRM, revise the proposed rule based on those comments, and provide the public with an additional opportunity to comment on the revised rulemaking. If it becomes final, the MMC rulemaking is not expected to go into effect until the initial TWIC roll out is complete. This time lapse will not cause a detrimental effect on security, as all credentialed mariners will still need to comply with the TWIC requirements and compliance deadlines set forth in this final rule.

II. Final Rule

Under this final rule, DHS, through the Coast Guard and TSA, requires all credentialed merchant mariners and individuals with unescorted access to secure areas of a regulated facility or vessel to obtain a Transportation Worker Identification Credential (TWIC).

A. Coast Guard Provisions

Owners/operators of MTSA-regulated vessels, facilities, and Outer Continental Shelf (OCS) facilities will need to change their existing access control procedures to ensure that merchant mariners and any other individual seeking unescorted access to a secure area of their vessel or facility has a TWIC.

B. TSA Provisions

Workers must provide biographic and biometric information to apply for a

TWIC and pay a fee of \$107–\$159 to cover all costs associated with the TWIC program. A TWIC applicant must complete a TSA security threat assessment and will be disqualified from obtaining a TWIC if he or she has been convicted or incarcerated for certain crimes within prescribed time periods, lacks legal presence and/or authorization to work in the United States, has a connection to terrorist activity, or has been determined to lack mental capacity.

All applicants have the opportunity to appeal a disqualification, and may apply to TSA for a waiver if disqualified for certain crimes or mental incapacity, or are aliens in Temporary Protected Status (TPS). Applicants who seek a waiver and are denied may seek review by an administrative law judge (ALJ). In addition, applicants who are disqualified under § 1572.107 may seek ALJ review of the disqualification.

A security threat assessment is valid for five years. Therefore, in most cases, a TWIC is valid for five years unless a disqualifying event occurs. If an applicant obtains a TWIC based on a comparable threat assessment under § 1572.5(e), the TWIC will expire five years from the date on the credential associated with the comparable threat assessment. To renew a TWIC, the renewal applicant must provide new biographic and biometric information, complete a new threat assessment, and pay the fee to renew the credential.

C. Changes From NPRM

Each of the changes made from the NPRM to the final rule is summarized in Table 1 and discussed in detail following the table.

TABLE 1.—SUMMARY OF SIGNIFICANT CHANGES BETWEEN MAY 22, 2006 NPRM AND THIS FINAL RULE

Topic	NPRM	Final rule
Access control	Visual identity badge and reader (with biometric verification and validity check at facility/vessel based on MARSEC level).	Visual identity badge; Coast Guard will conduct periodic checks of biometric and validity (second rule for reader requirements).
Escorted access	Definition only	Definition modified to clarify that in restricted areas (33 CFR 101.105), "escort" means a side-by-side escort; outside restricted areas, "escort" may consist of monitoring.
New hires	Not granted unescorted access to secure areas until successful completion of security threat assessment and card issuance.	Permitted to have limited access for 30 consecutive days if accompanied by TWIC-holder and additional requirements are met.
Passenger access area	Defined only for certain vessels (passenger, ferries, cruise ships).	Passenger access area remains and employee access area for certain vessels added (employee access areas do not apply to cruise ships).
TWIC Addendum and record-keeping requirements.	Included	Excluded.
Secure area	Definition only	Clarified definition's meaning in preamble, and revised part 105 to allow part 105 facilities to submit FSP amendment to change access control area.

TABLE 1.—SUMMARY OF SIGNIFICANT CHANGES BETWEEN MAY 22, 2006 NPRM AND THIS FINAL RULE—Continued

Topic	NPRM	Final rule
Lost/Stolen/Damaged cards	Access procedures defined in TWIC Addendum.	Specific requirements included in regulation.
AMS Committee members	Need TWIC	Need name-based check or a TWIC.
Vessels in foreign waters	No special provisions	Changed secure area definition to state that at certain specified times, U.S. vessels may not have any secure areas.
Emergency responders	Not specifically addressed	Not required to obtain a TWIC for emergency response.
Voluntary compliance	Offered	Not offered.
Compliance dates	12–18 months after final rule	Phased for facilities by each COTP zone. All mariners and vessels 20 months after the publication date of this final rule.
Disqualifying crimes	Same as those used for HME	Amended; new list will apply for both TWIC and HME.
Administrative law judge (ALJ) review.	Not included	May be used for waiver denials and disqualifications under § 1572.107.
Immigration standards	Limited ability for non-U.S. citizens to obtain TWICs.	Expanded to cover foreign maritime students, and certain professionals and specialists on restricted visas; permitting aliens in TPS to apply for a waiver.
Mental incapacity	Could only be waived by showing court order or letter from institution.	Waiver broadened to allow for “case-by-case” determinations.
Fee	\$95–\$149; card replacement fee \$36.	\$107–\$159; card replacement fee \$36, but requesting comment on increasing this fee to \$60.

1. Changes From Coast Guard's Proposed Rule

Coast Guard is changing several sections of the proposed rule as a result of comments received and additional analysis. These changes include: (1) Changing the access control procedures to be used with TWICs by removing the reader requirements; (2) revising and clarifying the definition of the term “escorting;” (3) adding provisions allowing for access for individuals who are new hires and who have applied for, but not yet received, a TWIC; (4) adding a provision to allow for limited, continued unescorted access for those individuals who report their TWIC as lost, damaged, or stolen; (5) adding a provision to create “employee access areas” aboard passenger vessels and ferries; (6) removing the proposed requirement to submit a TWIC Addendum and keep additional records regarding who has been granted access privileges; (7) adding a provision to allow certain facilities to designate smaller portions of their property as their secure area via an amendment to their facility security plan; (8) removing the proposed requirement for all AMS Committee members to hold a TWIC; (9) changing the definition of secure area to state that, at certain times, U.S. vessels may not have any secure areas; (10) adding a provision to allow emergency responders to have unescorted access without a TWIC during emergency situations; (11) removing the provision allowing for voluntary compliance for those vessels and facilities not otherwise required to implement the TWIC requirements; and (12) revising the compliance dates for owners/operators of vessels and facilities.

(a). Reader Requirements

After reviewing the comments (which are summarized below), we determined that implementing the reader requirements as envisioned in the NPRM would not be prudent at this time. As such, we have removed the reader requirements from the final rule, and will be issuing a subsequent NPRM to address these requirements. That NPRM will address many of the comments and concerns regarding technology that were raised in the below-summarized comments. We will, however, continue to require the use of the TWIC. As stated in the NPRM, there are considerable security benefits to be gained from a TWIC, even in the absence of reader usage. The TWIC provides greater reliability than existing visual identity badge systems because it presents a uniform appearance with embedded features on the face of the credential that make it difficult to forge or alter. When presented with a TWIC, security personnel familiar with its security features are immediately able to notice any absence or destruction of these features, making it less likely that an individual will be able to gain unescorted access to secure areas using a forged or altered TWIC. Additionally, the Coast Guard will conduct unannounced checks of the cards while visiting facilities and vessels. The Coast Guard will use handheld readers to check the biometrics on the card against the person presenting the card. These unannounced checks are an important component of the security efforts at the ports.

(b). “Escorting”/“Unescorted Access”

We have amended the definition of escorted access to clarify our intent. Namely, that the distinction between escort and unescorted access are to serve as performance standards, rather than strict definitions. We expect that, when in an area defined as a restricted area in a vessel or facility security plan, escorting will mean a live, physical side-by-side escort. Whether it must be a one-to-one escort, or whether there can be one escort for multiple persons, will depend on the specifics of each vessel and/or facility. We will provide additional guidance on what these specifics might be in a Navigation and Vessel Inspection Circular (NVIC). Outside of restricted areas, however, side-by-side escorting is not required, so long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual “under escort” be found in an area where he or she has not been authorized to go or is engaging in activities other than those for which escorted access was granted. Again, we will provide additional guidance with more specifics in a NVIC.

(c). New Hires

We have added a new section within parts 104, 105, and 106 to provide owners/operators with the ability to put new hires to work once new hires have applied for their TWIC and an initial name-based check is completed. In order to ensure adequate security for the vessel and facility during this period, these provisions allow new hires to have access to secure areas for up to 30 consecutive days, so long as they pass a TSA name based check and are

accompanied by another employee with a TWIC. If TSA does not act upon a TWIC application within 30 days, the Coast Guard may further extend access to secure areas for another 30 days. Additional guidance on the manner in which new hires may be accompanied will be issued by the Coast Guard. The guidance will be in the form of a NVIC that considers vessel or facility size, crew or staff size, vessel or facility configuration, the number of TWIC holders, and other appropriate factors, or by making a determination on a case-by-case basis. For example, in some instances, where the operating environment of the vessel is such that there is a small crew, and there is a 24-hour live watchstand while underway, we expect to view the new hires as accompanied when the vessel owner/operator ensures that the security measures for monitoring and access control included within their Coast Guard-approved security plans are implemented. As the operating environment increases or becomes more complex, such as might be the case when Certain Dangerous Cargoes (CDCs) are present, we expect to require additional security measures to ensure that the new hires are, in fact, accompanied by an individual with a TWIC. Similar guidance will also be in place for larger vessels, as well as for facilities and OCS facilities. The NVIC will be released in the near future.

In order to take advantage of this new hire provision, the following procedures must be followed:

(1) The new hire will need to have applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process and paying the user fee. He or she cannot be engaged in a waiver or appeal process. The owner or operator must have the new hire sign a statement affirming this.

(2) The owner or operator or the security officer must enter the following information on the new hire into the Coast Guard's Homeport Web site (<http://homeport.uscg.mil>):

(i) Full legal name, including middle name if one exists;
(ii) Date of birth;
(iii) Social security number (optional);
(iv) Employer name and 24 hour contact information; and
(v) Date of TWIC enrollment;

(3) The new hire must present an identification credential that meets the requirements of § 101.515 of this subchapter; and

(4) There must be no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the owner or operator or Facility Security

Officer (FSO) must not have been informed by the cognizant COTP that the individual poses a security threat.

This provision only applies to direct hires of the owner/operator; it cannot be used to allow temporary unescorted access to contractors, vendors, longshoremen, truck drivers (unless they are direct employees of the owner/operator), or any other visitor. This provision does not apply if the new hire is a Company, Vessel, or Facility Security Officer, or is otherwise tasked with security duties as a primary assignment.

In order for the Coast Guard and TSA to verify that a new hire who is awaiting TWIC issuance passes an initial security review, this provision includes a requirement for the owner, operator, Vessel Security Officer (VSO) or FSO to enter new hire identifying information into the Coast Guard's Homeport web page. The Homeport web page is a secure location capable of communicating sensitive security information such as Vessel Security Plans (VSP) and Facility Security Plans (FSP) between industry and the Coast Guard. The Homeport web page address is <http://homeport.uscg.mil>. Homeport will then interface with the TSA system, and if a match to an enrollment record can be made, the TSA system will pass back to Homeport the result of the initial name-based check. If the result is that the new hire has been cleared, the owner/operator/security officer can put the new hire to work under the provisions of this section and any guidance provided by the Coast Guard in a forthcoming NVIC.

TSA will begin the security threat assessment process as soon as the enrollment record is complete. Generally, TSA can complete an initial security review within 48–72 hours based on all of the information provided during enrollment. Thus, in some cases (where the new hire information is entered into Homeport three or more days following enrollment), the owner/operator/security officer will not have to wait long before finding out if an individual has cleared the initial name check. We expect that Homeport will be able to notify owners/operators/security officers, via e-mail, when it has received an update on any of the new hires entered by that owner/operator/security officer, which will alleviate any need for them to continuously check in with Homeport.

The new hire must have applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process and paying the user fee. The owner/operator must have the new hire sign a statement affirming the

enrollment, payment, and that the new hire is not involved in an appeal or waiver application. The owner/operator must retain this statement until the new hire receives a TWIC. The statement must be produced if the Coast Guard requests it during an inspection or investigation. The new hire must also present to the owner or operator a form of identification that meets the standard set in 33 CFR 101.515.

It is also important to note here that a new hire may be initially cleared to work in the secure area under the provisions of this section, but be disqualified from receiving a TWIC when the full threat assessment is complete. The results of the criminal history records check (CHRC) generally will not be fully adjudicated within three days, and if the adjudication reveals a disqualifying criminal history, the new hire will not be cleared to receive a TWIC.

The owner/operator of regulated vessels or facilities is required to accompany new hires in secure areas, which includes monitoring new hires while they are in restricted areas of the vessel or facility. Monitoring has the same meaning here as found in §§ 104.285, 105.275, and 106.275 of 33 CFR chapter I, subchapter H.

We are also requiring owners/operators of regulated vessels and facilities to determine that their new hires need access to secure areas immediately in order to prevent adverse impact to the operation of the vessel or facility. Owners and operators must identify that a hardship exists to their operations if their new hires are not allowed access. This adverse impact is not the impact of simply providing escorts for new hires, but must be adverse impacts to the business itself from not being able to employ new hires immediately in secure areas without escort.

Owners and operators of regulated vessels and facilities must be assured that there are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC. This information can come through the normal hiring process, reference checks, or interviews. Also, if the Coast Guard, through its Captain of the Port (COTP), has informed the owner/operator that the new hire poses a security threat, the new hire may not have unescorted access to secure areas of the vessel or facility. Only individuals who pass a threat assessment and are issued a TWIC may have unescorted access to secure areas of the vessel or facility.

(d). Access for Individuals With Lost/Stolen TWICs

Under the NPRM, we proposed requiring owners/operators to include alternative security procedures in the TWIC Addenda. These alternative procedures were to be used in various situations, such as when individuals needed unescorted access to secure areas but had lost their TWIC, had it stolen, or simply forgotten it that day. As discussed below, we removed the TWIC Addendum requirement from the final rule, but we wanted to include a provision to allow TWIC holders to continue, for a short period, to have unescorted access to secure areas after reporting their TWICs as lost, damaged, or stolen. As a result, this final rule includes specific procedures for owners/operators to use in the case of lost, damaged, or stolen TWICs. This procedure includes having the individual report his/her card as lost, damaged, or stolen to the TWIC Call Center and checking another form of identification that meets 33 CFR 101.515, provided there are no other suspicious circumstances that would cause an owner/operator to question the veracity of the individual. In order to prevent this procedure from becoming a significant loophole in the TWIC regulation, we require that the individual be known to have had a valid TWIC and to have previously been granted unescorted access, and have limited the use of the procedure to seven (7) consecutive calendar days. This should provide enough time for the replacement card to be produced and shipped to the nearest enrollment center, and for the individual to travel to that center to pick up the replacement card.

(e). "Employee Access Areas"

We intended for the term "passenger access area" to capture those employees whose jobs are necessary solely for the entertainment of the passengers of the vessel, such as musicians, wait staff, or casino employees on a passenger vessel. Upon reviewing comments, however, we realized that there are a variety of employees who may need to enter non-passenger spaces, such as the galley, who would be included under TWIC's applicability merely because of their need to enter these areas. As such, we are adding a definition for "employee access areas," for use only by passenger vessels and ferries. An employee access area is a defined space within the access control area of a ferry or passenger vessel that is open to employees but not passengers. It is not a secure area and does not require a TWIC for unescorted access. It may not include any areas

defined as restricted areas in the vessel security plan (VSP). Note, however, that any employee that needs to have unescorted access to areas of the vessel outside of the passenger or employee access areas will need to obtain a TWIC.

(f) TWIC Addendum and Recordkeeping Requirements

We removed the TWIC Addendum requirement from the final rule when we determined that the reader requirements would be delayed until a subsequent rulemaking. The purpose of the TWIC Addendum was to allow the owner/operator to explain how the readers would be incorporated into their overall access control structure, within the standards provided in the NPRM. With the removal of the reader requirements from this final rule, we feel it is appropriate to also remove the TWIC Addendum requirement. Additionally, because we envision the TWIC Addendum to be a part of the subsequent rulemaking on reader requirements, we felt it would be overly burdensome to also require a TWIC Addendum at this point in time.

The recordkeeping requirements related to TWIC implementation have also been removed from the final rule. We had proposed the requirements because we believed they could be satisfied by using the TWIC readers, which were also proposed. Due to our decision to remove the reader requirements from this final rule, it makes sense to also remove the recordkeeping requirements that were intrinsically tied to those readers.

(g). Secure Area

We did not intend for the terms "secure area" and "restricted area" to be read as meaning the same thing. Restricted areas are defined already in the MTSA regulations as "the infrastructure or locations identified in an area, vessel, or facility security assessment or by the operator that require limited access and a higher degree of security protection." (33 CFR 101.105) Additionally, those regulations spell out certain areas within vessels and facilities that must be included as restricted areas (*see* 33 CFR 104.270, 105.260, and 106.265). This final rule defines "secure area" as meaning the area over which an owner/operator has implemented security measures for access control. In other words, the secure area would be anything inside the outer-most access control point of a facility, and it would encompass the entirety of a vessel or OCS facility.

We adopted this definition after much consideration, including consideration of making only restricted areas secure

areas. We ultimately abandoned this option, however, when we realized that equating the restricted area to the secure area would have required that the readers and biometric verification be used at the entry points of each restricted area. Because some facilities and vessels have multiple restricted areas that are not always contiguous, this would have likely meant that many owners/operators would have needed more than one reader, increasing their compliance costs. Additionally, the process of repeated biometric identification could have interfered with the operations of facilities and vessels. Finally, we determined that there are areas within some facilities that are not required to be restricted areas that should be deemed secure areas, such as truck staging areas, empty container storage areas, and roads leading between the facility gates and the pier. Allowing persons who have not been through the security threat assessment or are not escorted to have access to these areas could provide them with the opportunity to access the non-restricted areas of the facility to perpetrate a transportation security incident (TSI). Pushing the secure area out beyond the restricted area makes the event of an intentional TSI less likely. As a result, we decided to define the secure area as the "access control area," thus limiting the number of readers required, as well as the number of times biometric verification would need to take place, and providing for the necessary level of security outside of restricted areas. We note, however, that facility owners/operators have the discretion to designate their entire facility as a restricted area. In this situation, the restricted area and secure area would be one and the same.

We recognize that many facilities may have areas within their access control area that are not related to maritime transportation, such as areas devoted to manufacturing or refining operations, and were only included within the FSP because the owner/operator did not want to have to install additional access control measures to separate the non-maritime transportation related portions of their facility from the maritime transportation related portions. Given the new obligations of this TWIC final rule, however, these owners/operators may wish to revisit this decision. As such, we are giving facility owners/operators the option of amending their FSP to redefine their secure area, to include only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation

security incident. These amendments must be submitted to the cognizant COTP by July 25, 2007.

We realize that there may be some owners and operators of vessels that would like the same option. However, vessels present a unique security threat over facilities in that they may not only be targets in and of themselves, but may also be used as a weapon. Due to this fact, we will continue to define the entire vessel as a "secure area," making exception only for those special passenger and employee access areas which are discussed above. Vessel owners/operators need not submit an amendment to the VSP in order to implement these special areas, however they may do so, following the procedures described in part 104.

(h). U.S. Vessels in Foreign Waters

Due in part to the unique operating requirements imposed on U.S. Offshore Supply Vessels (OSVs) and Mobile Offshore Drilling Units (MODUs) when operating in support of OCS facilities in foreign waters, we determined that we must change some language from the proposed rule. As such, we are adding a provision to the definition of secure area in § 101.105 that states that U.S. vessels operating under the waiver provision in 46 U.S.C. 8103(b)(3)(A) or (B) have no secure areas. These waiver provisions allow U.S. vessels to employ foreigners as crew in certain circumstances. The effect of this change is to exempt these vessels from the TWIC requirement while they are operating under the referenced waivers. As soon as the vessel ceases operating under these waiver provisions, it will be deemed to have secure areas as otherwise defined, and TWIC provisions will apply.

(i). Area Maritime Security (AMS) Committee Members

The NPRM proposed requiring all members of AMS Committees to have a TWIC. We recognize that large numbers of the members will either (1) already have a TWIC, due to their role within the security organization of a facility, or (2) already have undergone some type of comparable background screening due to their position as a Federal, State, or local law enforcement official. After further consideration, we believe that anyone not falling into one of these categories could be discouraged from volunteering to sit on an AMS Committee, due to the cost of obtaining a TWIC. This could have a detrimental effect on the AMS Committee, as there may be individuals who are experts in security who would be (and in some cases already are) valuable parts of AMS

Committees, who would opt out of sitting on the Committee rather than assume the cost of obtaining a TWIC. Therefore, we have changed the final rule to allow AMSC members to serve on the AMSC after the completion of a name-based terrorist check from TSA. If an AMSC member requires unescorted access to secure areas of vessels or facilities they will be required to obtain a TWIC. If, however, they do not require unescorted access, but do need access to SSI, they must first pass a TSA name based check at no cost to the AMSC member. The Federal Maritime Security Coordinator for the member's particular AMSC (*i.e.* COTPs) will forward the names of these individuals to TSA or Coast Guard Headquarters for clearance prior to sharing SSI with these members.

(j). Emergency Responders

We added a provision within 33 CFR 101.514 to allow State and local emergency responders to gain access to secure areas without a TWIC during an emergency situation. Not all emergency responders will fall into the category of State or local officials. We feel it is imperative that these individuals be allowed unescorted access to secure areas in an emergency situation. Emergency responders who are not State or local officials are encouraged to apply for a TWIC. Under the existing access control requirements of 33 CFR 105.255, the owner or operator has documented procedures for checking credentials prior to allowing access and will maintain responsibility for all those granted access to a vessel or facility, even in an emergency situation.

(k). Voluntary Compliance

The provisions that would have allowed vessel and facility owners/operators to implement voluntary TWIC programs have been removed. These provisions have been eliminated due to the fact that neither TSA nor the Coast Guard can, at this time, envision being in a position to approve voluntary compliance before the full TWIC program, (*i.e.*, reader requirements) is in place. We will keep it in mind, however, as we develop our NPRM to repropose reader requirements.

(l). Compliance Dates

We have also revised the compliance dates slightly. Vessels will now have 20 months from the publication date of this final rule to implement the new TWIC access control provisions. Facilities will still have their compliance date tied to the completion of initial enrollment in the COTP zone where the facility is located. This date will vary, and will be

announced for each COTP zone at least 90 days in advance by a Notice published in the **Federal Register**. The latest date by which facilities can expect to be required to comply will be September 25, 2008. Additionally, mariners will not need to hold a TWIC until September 25, 2008. Mariners may rely upon their Coast Guard-issued credential and a photo ID to gain unescorted access to secure areas to any facility that has a compliance date earlier than September 25, 2008.

2. Changes From TSA's Proposed Rule

TSA is changing several sections of the proposed rule as a result of comments received, new legislation, and additional analysis. The changes include: (1) Establishing procedures for review of waiver denials by an ALJ; (2) applying the hazmat and TWIC appeal procedures to air cargo personnel; (3) amending the list of disqualifying criminal offenses; (4) expanding the group of aliens who meet the immigration standards; (5) amending the waiver standards for applicants disqualified due to mental incapacity; (6) amending the fees for TWIC; (7) revising the standard for drivers licensed in Mexico and Canada who transport hazardous materials into and within the United States; and (8) modifying the prohibitions on fraudulent use or manufacture of TWIC or access control procedures.

(a). Review by Administrative Law Judge

We noted in the NPRM that if legislation was enacted after publication of the final rule to require review by an Administrative Law Judge of the denial of waiver requests by TSA, we would include such a statutory mandate in the final rule. *See* 71 FR at 29421. The Coast Guard and Maritime Transportation Act of 2006, Pub. L. 109-241, was enacted on July 11, 2006. Section 309 of this Act requires the Secretary of Homeland Security to establish an ALJ review process for individuals denied a waiver by TSA. Accordingly, we are including the ALJ review procedures in new § 1515.11.

The ALJ review process set forth under § 1515.11 does not alter the substantive criteria under which TSA will grant or deny a waiver. Therefore, this provision constitutes a rule of agency procedure and may be implemented without prior notice and comment under the Administrative Procedure Act, 5 U.S.C. 553(b)(A). *See Hurson Assoc. Inc., v. Glickman*, 229 F.3d 277 (D.C. Cir. 2000) (rule eliminating face-to-face process in agency review of requests for approval

was procedural and not subject to notice-and-comment rulemaking).

The new legislation requires ALJ review to be available for denials of waivers. Under the rules waivers are not available for determinations under § 1572.107 that an applicant poses a security threat, which usually is based on an intelligence-related check involving classified information.

However, we have considered that there appears to be an intent that we provide for an ALJ review of such determinations, considering, for example, that the statute provides for ALJ review of classified information, which rarely is relevant to waivers under the current rules. We have also considered that the decision to determine whether an applicant poses a threat under § 1572.107 is largely a subjective judgment based on many facts and circumstances. The same is true for the decision to grant or deny a waiver of the standards in §§ 1572.103 (criminal offenses), aliens who are in TPS under 1572.105, or 1572.109 (mental capacity). Accordingly, we are providing for ALJ review of both a determination that the applicant does not meet the standards in § 1572.107, and a denial of a waiver of certain standards in §§ 1572.103, 1572.105, and 1572.109.

An applicant who has received an Initial Determination of Threat Assessment based on § 1572.107 may first appeal that determination using the procedures in new § 1515.9. If after that appeal TSA continues its determination that the applicant is not qualified, the applicant may seek ALJ review under § 1515.11.

On the other hand, the determination that an applicant does or does not have a disqualifying criminal offense listed in § 1572.103, immigration status in § 1572.105, or mental capacity described in § 1572.109, largely involves an analysis of the legal events that have occurred. Such analyses depend mainly on review of legal documents. We have retained in § 1515.5 the paper hearing process for the appeal of an Initial Determination that an applicant is not qualified under those sections. At the end of that appeal, if TSA issues a Final Determination that the applicant is not qualified under one of those sections, the applicant may seek review in the Court of Appeals. At any time, however, the applicant may seek a waiver of certain standards in those sections on the basis that, notwithstanding a lack of qualification, the applicant asserts that he or she does not pose a security threat and thus seeks to waive the subject standards. The applicant initiates the request for a waiver using the

procedures in § 1515.7. If a waiver is not granted, the applicant may seek review by an ALJ under § 1515.11.

For consistency, we are providing the same review processes for hazardous materials endorsement (HME) applicants that we are providing for TWIC applicants.

Paragraph 1515.11(a) of this new section specifies that the new process applies to applicants who are seeking review of an initial decision by TSA denying a request for a waiver under § 1515.7 or who are seeking review of a Final Determination of Threat Assessment issued under § 1515.9.

Section 1515.11(b) allows the applicant 30 calendar days from the date of service of the determination to request a review. The review will be conducted by an ALJ who possesses the appropriate security clearances to review classified information. The rule sets forth the information that the applicant must submit. This section clarifies that the ALJ may only consider evidence that was presented to TSA at the time of application in the request for a waiver or the appeal. If the applicant has new evidence or information to support a request for waiver, the applicant must file a new request for a waiver under § 1515.7 or a new appeal under § 1515.9 and the pending request for review will be dismissed. Section 1515.11 provides detailed requirements for the conduct of the review, such as requests for extension of time and duties of the ALJ.

In accordance with the Coast Guard and Maritime Transportation Act, this section provides for ALJ review of classified information on an *ex parte*, in camera basis and consideration of such information in rendering a decision if the information appears to be material and relevant.

Paragraph 1515.11(f) provides that within 30 calendar days after the conclusion of the hearing, the ALJ will issue an unclassified decision to the parties. The ALJ may issue a classified decision to TSA. The ALJ may decide that the decision was supported by substantial evidence on the record or that the decision was not supported by substantial evidence on the record. If neither party requests a review of the ALJ's decision, TSA will issue a final order either granting or denying the waiver or the appeal.

Paragraph 1515.11(g) describes the process by which a party may petition for review of the ALJ's decision to the TSA Final Decision Maker. The TSA Final Decision Maker will issue a written decision within 30 calendar days after receipt of the petition or receipt of the other party's response.

The TSA Final Decision Maker may issue an unclassified opinion to the parties and a classified opinion to TSA. The decision of the TSA Final Decision Maker is a final agency order.

Paragraph 1515.11(h) states that an applicant may seek judicial review of a final order of the TSA Final Decision Maker in accordance with 49 U.S.C. 46110, which provides for review in the United States Court of Appeals. Under sec. 46110 a party has 60 days after the date of service of the final order to petition for review.

(b). Appeal Procedures for Air Cargo Personnel

In the final rule we are adding the appeal procedures that currently apply to air cargo workers codified at 49 CFR parts 1540 to 1515. In the NPRM TSA stated that it may use the procedures in part 1515 for other security threat assessments, such as for air cargo personnel. See 71 FR at 29418. At that time the air cargo proposed rule had been published but was not yet final, and it proposed to use appeal procedures that were essentially the same as for HME applicants. The air cargo rule has now been made final. See 71 FR 30478 (May 26, 2006). Because part 1515 was not yet final in the air cargo rule, we placed the appeal procedures for the air cargo security threat assessment into part 1540 subpart C, along with other procedures that apply to air cargo threat assessments. In a further effort to harmonize security threat assessments, we are now moving the appeal procedures for air cargo personnel to part 1515. For consistency with the TWIC and HME processes we are providing for review by an ALJ as described above.

We are also revising part 1540 subpart C to harmonize more with part 1572. Thus, we are replacing "individual" with "applicant" to refer to the person who is applying for a security threat assessment. We are also revising § 1540.205 to read essentially the same as § 1572.21 for TWIC, because it serves the same function. Note that while the procedures for TWIC refer to CHRCs and other checks, the procedures for air cargo personnel refer only to intelligence-related checks, because they are not subject to the other checks conducted on TWIC applicants.

(c). Disqualifying Criminal Offenses.

In this final rule, the list of criminal acts that disqualify an applicant from holding an HME under 49 CFR 1572.103 now applies to TWIC applicants. We believe equal treatment for transportation workers is appropriate and consistent with the pertinent

statutory requirements. The standards for the HME rule were mandated by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) Pub. L. 107–56, 115 Stat. 272 (October 25, 2001). It provides that TSA conduct a security threat assessment on applicants to determine if they pose a “security risk.” The USA Patriot Act was enacted shortly after and in response to the terrorist attacks on the United States on September 11. As a result, we interpreted the language “security risk” to mean a risk of terrorism or terrorist activity. Nothing in the statute or the legislative history of the USA Patriot Act contradicts this reading of the language. MTSA, enacted a year later, requires a security threat assessment to determine whether an applicant poses a “terrorism security threat.” We believe the security threat assessment required under MTSA is the same threat assessment required under the USA Patriot Act, even though the actual language differs slightly.

In addition, TSA is making administrative and substantive changes to this section. In the NPRM, TSA indicated that it was considering changing the list of disqualifying crimes and asked for comment on the list. TSA received significant comments from Congress and others suggesting that the list of disqualifying crimes is overly broad, and that some crimes had more of a nexus to terrorism than others. 152 Cong. Rec. 2120 (2006). *See also* Comments of House Committee on Homeland Security on TSA and Coast Guard’s Rule to Implement TWIC, July 6, 2006. TSA has evaluated the list of disqualifying crimes and decided to fine tune the list to better reflect crimes that are more likely to result in a terrorism security risk or a transportation security incident, and thus should disqualify an applicant from receiving a TWIC.

TSA is making a substantive change to this section concerning the crimes of treason, sedition, espionage, and terrorism listed in § 1572.103(a), which are permanently disqualifying. Applicants convicted of these crimes are not eligible for a waiver. As we proposed to do in the NPRM, TSA is adding conspiracy to commit these crimes to the list of crimes that are not subject to a waiver request. TSA has determined that a conviction of conspiracy to commit espionage, treason, sedition, or terrorism is indicative of a serious, ongoing, unacceptable risk to security and should not be waived under any circumstances.

TSA is changing the language in (a)(4) from “a crime listed in 18 U.S.C. Chapter 113B—Terrorism” to “a federal

crime of terrorism as defined in 18 U.S.C. 2332b(g)” or conspiracy to commit such crime, or comparable State law. Section 2332b(g) is a definitional list that is broader and more explicit than the crimes punished directly in Chapter 113B. We are making this change to more accurately capture all pertinent terrorism-related crimes. Although we intended to be as inclusive as possible with the previous language, experts at the Department of Justice advise that the new language more accurately captures the relevant criminal acts. TSA is adding felony bomb threat in paragraph (a)(9) as a permanent disqualifier including maliciously conveying false information concerning the deliverance, placement, or detonation of an explosive or other lethal device against a state or government facility, public transportation system or an infrastructure facility. TSA is including this crime because it is, in essence, a threat to commit an act of terrorism. We note that we have disqualified an applicant with such crime under the authority of current paragraph (b)(6) dishonesty, misrepresentation, or fraud. To be clear that this crime is a permanent disqualifier, we are adding it as an independent offense in § 1572.103(a)(9). This offense includes making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportation system, or an infrastructure facility.

Paragraph 1572.103(a)(9) is based in part on conduct prohibited by several federal crimes. The first is 18 U.S.C. 844(e), which is found in chapter 40 (Explosive Materials) of the federal criminal code. Section 844(e) criminalizes the use of the mail, telephone, or other instrument of interstate or foreign commerce to willfully make any threat or maliciously convey false information knowing the same to be false, concerning an attempt to kill, injure, or intimidate any individual or unlawfully damage or destroy any building, vehicle, or other real or personal property by means of an explosive. This crime is already disqualifying under paragraph (a)(7). For inclusion in the list of disqualifying crimes, TSA modified this description to broaden it beyond a threat made through an instrument of interstate or foreign commerce. This change provides a disqualification for purely intrastate conduct that results in a felony

conviction under State law. TSA also modified the wording found in section 844(e) to include threats of use of lethal weapons in addition to fire and explosives, such as biological, chemical, or radiological weapons. Threats to use these weapons are prohibited by other sections of the federal criminal code. *See, e.g.*, 18 U.S.C. 175 (Biological weapons); 18 U.S.C. 229 (Chemical Weapons); and 18 U.S.C. 2332h.

TSA has revised the language of paragraph (b) to clarify that the crimes listed are disqualifying if either of the following are true: (1) The applicant’s date of conviction is within seven years of the date of application; or (2) the applicant was incarcerated for that crime and was released from incarceration within five years of the date of application.

TSA is adding the offense of fraudulent entry into seaport secure areas to the list of interim disqualifiers. This is a new provision in 18 U.S.C. 1036 that we believe is particularly relevant to this rulemaking and any TWIC applicant.

TSA is also clarifying in paragraph (b)(2)(iii) that money laundering is an interim disqualifier because it is encompassed under the crimes of dishonesty and fraud and can be a means of funding terrorism. It is known that criminals obtain money from the illegal sale of drugs, firearms and other contraband, launder the money to hide its origin and then funnel this money to terrorist groups. The money laundering disqualifier is limited to convictions where the laundering was for proceeds of other disqualifying criminal activities such as drugs or weapon sales.

TSA is also clarifying that welfare fraud and passing bad checks will not be considered crimes of dishonesty, fraud, or misrepresentation for purposes of paragraph (b)(2)(iii). In some states, conviction for passing a bad check of \$100 is a felony and so would be disqualifying for an HME or TWIC applicant. Similarly, a conviction for welfare fraud can be a felony under state law, depending on the circumstances of the case. TSA believes that these crimes generally do not have a nexus to terrorism and therefore should not be disqualifying under MTSA.

TSA is moving the definitions of “explosive,” “firearm,” and “transportation security incident” from § 1572.3 to § 1572.103, where the terms are used. This should help to eliminate uncertainty about the crimes that are disqualifying. In addition, TSA is adopting clarifying language concerning the kind of activity that constitutes a “transportation security incident.” As required in § 7105 of SAFETEA-LU,

codified at 47 U.S.C. 5103a(g)(3), the definition now makes clear that nonviolent labor-management activity is not considered a disqualifying offense.

The list of disqualifying crimes in § 1572.103 applies equally to TWIC and HME applicants, thus the amendments apply to both.

(d). Immigration standards

The NPRM was drafted to permit non-resident aliens in the U.S. with unrestricted authorization to work here to apply for and obtain a TWIC. As a result of comments and the relatively common employment of foreign specialists in certain maritime job categories who do not have “unrestricted” work authorization, we are expanding the group of aliens who can apply to include certain restricted work authorization categories.

For purposes of this discussion, it is helpful to explain that there are two categories of U.S. visas: immigrant and nonimmigrant. As provided in the immigration laws, an immigrant is a foreign national who has been approved for lawful permanent residence in the United States. Immigrants enjoy unrestricted eligibility for employment authorization. Nonimmigrants, on the other hand, are foreign nationals who have permanent residence outside the United States and who are admitted to the United States on a temporary basis. Thus, immigrant visas are issued to qualified persons who intend to live permanently in the United States. Nonimmigrant visas are issued to qualified persons with permanent residence outside the United States, but who are authorized to be in the United States on a temporary basis, usually for tourism, business, study, or short-or long-term work. Certain categories of lawful nonimmigrant visas or status allow for restricted employment authorization during the validity period of the visa or status.

TSA has carefully reconsidered the immigration standards we proposed in the NPRM in light of the comments we received relating to immigration status and our own ongoing analysis. As a result, we are amending the immigration standards for TWIC and HME applicants. The critical issues we examined and on which we rely to determine whether an alien should be permitted to apply for a TWIC or HME are: (1) The statutory language regarding immigration status; (2) the degree to which TSA can complete a thorough threat assessment both initially and perpetually on the applicant; (3) the duration of the applicant’s legal status as of the date he or she enrolls and the degree to which we can control

possession of a TWIC once legal status ends; (4) the restrictions, if any, that apply to the applicant’s immigration status; (5) particular maritime professions that commenters stated often involve aliens; and (6) the checks done by the U.S. Department of State (State Department) or other federal agency relevant to granting alien status.

With respect to non-U.S. citizens, MTSA provides that an individual may not be denied a TWIC unless he or she may be denied admission to or removed from the United States under the Immigration and Nationality Act (8 U.S.C. 1101, *et seq.*), or “otherwise poses a terrorism security risk to the United States³.” 46 U.S.C. 70105(c). Under this final rule, all applicants for TWICs must be lawfully present in the country. Each of the permissible classes listed in § 1572.105 has, as a basis, lawful presence in the United States. Additionally, if the duration of an applicant’s legal status as of the date of enrollment does not meet or exceed the period of validity of the credential, five years, we have concerns about permitting the applicant to receive a TWIC⁴. Given the statutory language—that we may deny a TWIC to an applicant who “*may be denied admission to the United States or removed from the United States under the Immigration and Nationality Act*”—we believe it is not advisable and may be inconsistent with MTSA to issue a five-year credential to an individual whose known lawful status as of the date of enrollment is a much shorter time period. The statutory language reflects the evolving nature of immigration status and we believe it is a significant distinction that warrants particular treatment.

Changes to alien status occur frequently and are difficult to track accurately in real time and perpetually, both of which are necessary to ensure that a TWIC holder remains in legal

status. Where we can achieve a level of certainty that the applicant will not possess a TWIC longer than his or her lawful presence and commenters have indicated there is a need for certain short-term aliens to hold a TWIC, we will consider issuing them a credential.

Many aliens in lawful nonimmigrant status are not eligible to work in the United States or their employment authorization is restricted in some way, usually to the particular sponsoring employer or entity. With the exception of students in valid M–1 nonimmigrant status who are enrolled in the U.S. Merchant Marine Academy or a comparable State school and must complete vocational training, we do not believe it would be consistent with MTSA to permit lawful nonimmigrants that are ineligible to work or conduct business in the United States to apply for a TWIC. Also, if the employment restriction placed on the nonimmigrant generally prevents the individual from working in a maritime facility or vessel, we do not believe a TWIC should be granted. The final rule now lists the nonimmigrant classifications with restricted employment authorization that have a nexus to the maritime industry. Aliens in these nonimmigrant categories with restricted employment authorization may apply for a TWIC notwithstanding the fact that their immigration status may expire in less than five years, because we are requiring additional measures to ensure that the TWIC expires after the employment that requires unescorted access to secure areas ends.

The final rule now requires employers of TWIC holders who are lawful nonimmigrants with restricted authorization to work to retrieve the applicant’s TWIC when the job for which the nonimmigrant status was granted is complete. The employer in this situation should be well aware that the employment status has ended because the visa was issued to facilitate a specific job or employment with the employer. However, if an employer terminates the employment relationship with the alien working on a restricted visa, or that alien quits working for the employer, the employer is required to notify TSA within 5 days and provide the TWIC to TSA if possible. Additionally, all applicants must return their TWIC to TSA when they are no longer qualified for it, and a visa applicant’s TWIC expires when either the employment ends or the visa expires. These requirements should minimize the likelihood that an alien will continue to possess a TWIC and have unescorted access to secure areas

³ The governing statute for immigration standards for an HME (49 U.S.C. 5103a) requires TSA to “review relevant databases to determine the status of an alien under U.S. immigration law,” which provides TSA more discretion to determine whether an alien in a particular immigration class should hold an HME. In order to maintain consistent standards among transportation workers where possible, the immigration standards we are establishing in this final rule for TWIC applicants will also apply to HME applicants. However, as a threshold matter, HME applicants must first meet the standards to hold a commercial driver’s license promulgated by the U.S. Department of Transportation, which may include immigration status.

⁴ The TSA system is not currently programmed to issue credentials with varying expiration dates; all TWICs will expire five years from the date on which they were issued. We plan to explore modifying aspects of the TSA system as the program matures.

of the maritime industry after his or her legal status to do so expires.

The requirement to return a TWIC to TSA when the pertinent employment ends does not apply to employers of lawful nonimmigrants with unrestricted authorization to work or employers of unrestricted lawful nonimmigrants. Under the immigration laws, the status assigned to an alien carries with it the determination that the individual may work in the United States with or without restriction. Where the alien status includes employer sponsorship as a condition of legal presence, we believe it is appropriate to require the employer to return the credential to TSA once that relationship ends. However, in the cases of alien status that do not carry employment restrictions, we do not believe it is advisable at this time to require any employer action. The lawful nonimmigrant who is not under employment restriction may cease working for an employer and maintain legal status. Retrieving the TWIC at this point would not be appropriate. If the applicant loses lawful status, under the rule, he or she must report any disqualifying offense to TSA and surrender the TWIC. In addition, the enrollment record for each applicant contains contact information for employers, and if TSA determines that an applicant has lost legal status, we would generally have the information necessary to contact the employer and the TWIC holder.

To satisfy the second prong of MTSA's immigration status requirement, that a TWIC holder does not pose a terrorism security threat to the United States, TSA considers a variety of factors. TSA must be able to conduct a comprehensive threat assessment of the applicant. As in all of TSA's security threat assessment programs, we will conduct a comprehensive threat assessment of each applicant upon enrollment, and then will vet the applicants perpetually using appropriate databases throughout the five-year term of the TWIC. We consider the initial and perpetual vetting to be equally important in maintaining a high level of confidence in the TWIC population. To the extent that a full threat assessment cannot be completed on an applicant initially or perpetually, TSA has concerns about granting that applicant unescorted access to secure areas of maritime facilities and vessels.

Many immigration statuses change over time, and TSA generally is not in a position to perpetually vet the immigration status of an applicant. We are reluctant to provide a five-year TWIC under these circumstances unless

we achieve some level of control over the actual credential through the applicant's employer to minimize the likelihood that an alien who has lost lawful status keeps the credential.

A significant component of a comprehensive security threat assessment is a fingerprint-based criminal history records check for arrests, indictments, wants, warrants, and serious felony convictions. If we are unable to complete such a check because we cannot access the criminal records of the country in which an applicant has lived for many years, we have concerns that we cannot make an accurate assessment of the individual. Many U.S. workers commented on this fact, in some cases asserting that U.S. citizens are held to a higher standard than workers born abroad because of the inability to do a complete criminal records check on foreign-born applicants. We do not believe that this situation alone constitutes justification to deny non-citizens a TWIC, particularly since U.S. citizens may be born abroad, or spend substantial time abroad. However, it does give rise to a legitimate security concern. Consequently, we must make every effort to minimize the likelihood that someone with malicious intent can enter the United States legally or illegally, hide significant prior criminal or terrorist activity, and obtain unescorted access to secure areas of the maritime industry.

To reduce the likelihood that TWICs will be issued to someone with malicious intent, we are changing the immigration standards in a variety of ways to reduce those eligible for TWICs to only those individuals on whom the Department of State and/or DHS can perform an adequate security review. First, we are not permitting certain aliens in lawful nonimmigrant status with unrestricted employment authorization to apply for a TWIC. We are not permitting aliens in valid S-5 or S-6 lawful nonimmigrant status with unrestricted authorization to work in the United States to apply for a TWIC. Individuals who are in S-5 and S-6 lawful nonimmigrant status are informants providing information relating to criminal or terrorist organizations. Typically, individuals who are able to provide this kind of information to law enforcement personnel in the United States have been engaged in criminal or terrorist activity themselves. For this reason, we believe they pose a security risk and should not be granted a TWIC. Additionally, this status is granted to no more than 250 individuals per year, and so the likelihood that preventing these

individuals from applying for a TWIC would adversely impact a significant number of applicants or the maritime industry is virtually nonexistent. Finally, the S-5 and S-6 status requires frequent contact with U.S. law enforcement personnel for approximately three years, after which time the applicant may be recommended for lawful permanent resident status. After these individuals satisfy the conditions of their status and become lawful permanent residents, the risk they initially present would effectively be mitigated and they would be permitted to apply for a TWIC.

We do not believe it is advisable to permit lawful nonimmigrants in K-1 or K-2 status to apply for a TWIC. These individuals include the fiancés and minor children of fiancés of U.S. citizens. Their lawful status expires in just four months. We believe these individuals can be escorted under the final rule until they obtain permanent or other lawful status.

Aside from holders of the S-5 and S-6 and K-1 and K-2 statuses all lawful nonimmigrants with unrestricted authorization to work in the United States may apply for a TWIC.

Second, we are revising the rule to treat U.S. nationals, that is, principally American Samoans, as we treat U.S. citizens.⁵ We accomplished this change by adding a definition to the rule for "National of the United States," which means a citizen of the United States or an individual who owes permanent allegiance to the United States. This change is consistent with longstanding principles of immigration law and we believe would not introduce a security threat. Similarly, the final rule permits citizens of the Federated States of Micronesia, the Republic of the Marshall Islands, and Palau who have been admitted as nonimmigrants under the Compacts of Free Association between the United States and those countries to apply for a TWIC. The United States has entered into treaties with these countries that afford their citizens preferred treatment. For instance, citizens of these countries may reside indefinitely and work in the United States without restriction. Therefore, we believe it is appropriate to permit these individuals to apply for a TWIC.

Third, in response to many comments about the use of foreign professionals in the maritime industry for specialty work, we are permitting certain lawful

⁵ Note that Swains Island has been incorporated into American Samoa and thus does not need a separate reference. (48 USC 1662) In addition, this includes nationals of the Commonwealth of the Northern Mariana Islands.

nonimmigrants with restricted authorization to work in the United States to apply for a TWIC. There is a longstanding practice of employing non-U.S. citizens to complete specialized maritime tasks, such as maintaining vessel engines and motors. In addition, many international maritime companies transfer staff from abroad into the United States for short or long-term periods, and many of these individuals must work at maritime facilities or on vessels. Denying this segment of the industry the opportunity to apply for a TWIC could adversely impact maritime operations and economic vitality. However, to mitigate our concerns about the inability to complete a thorough initial and perpetual threat assessment on individuals who have not lived in the United States for any significant period of time and who are authorized to remain in the United States for less than five years, we are adding requirements for employers and affected workers to return the TWIC to TSA when the job is completed or the worker otherwise ceases employment with the company.

We received a comment concerning aliens who are religious personnel in valid R-1 lawful nonimmigrant status with restricted employment authorization. The commenter noted that vessel crew members may request spiritual guidance or religious services when their vessel docks at a port in the United States, and religious workers in valid R-1 status should be permitted to apply for a TWIC to board the vessel. Seafarer Welfare Advocates are eligible for TWICs as long as they meet the TWIC rulemaking eligibility requirements; however, there are no exemptions for aliens holding R-1 visas. We believe that individuals with R-1 visas can be escorted because any individual providing religious services to crew members on a vessel would be on board the vessel for relatively short periods of time and would most likely be in the company of TWIC holders during that time. While we do not believe that these individuals need to

hold a TWIC to carry out their religious or spiritual functions, they may apply and will be issued TWICs if they meet the eligibility requirements.

Fourth, we are permitting students of the United States Maritime Academy and comparable State maritime colleges in valid M-1 lawful nonimmigrant status to apply for a TWIC. These individuals clearly have a need for unescorted access to maritime facilities and vessels as they complete their vocational training in the United States.

Fifth, we are adding individuals who are in TPS to the group of applicants who may apply for a waiver. Temporary Protected Status is a temporary immigration status granted to eligible nationals of designated countries. The Secretary may designate a country for TPS when it is determined that (1) there is an ongoing armed conflict in the state and, due to that conflict, return of nationals to that state would pose a serious threat to their personal safety; (2) the state has suffered an environmental disaster resulting in a substantial, temporary disruption of living conditions, the state is temporarily unable to handle adequately the return of its nationals, and the state has requested TPS designation; or (3) there exist other extraordinary and temporary conditions in the state that prevent nationals from returning in safety.

TPS beneficiaries are not required to leave the United States and may obtain work authorization for the initial TPS period and for any extensions of the designation. TPS does not automatically lead to permanent resident status. A TPS designation may be effective for a minimum of 6 months and a maximum of 18 months. Before the end of the TPS designation period, the conditions that gave rise to the TPS designation are reviewed. Unless a determination is made that those conditions are no longer met, the TPS designation will be extended for 6, 12, or 18 months. If the conditions that led to the TPS designation are no longer met, the TPS designation is terminated. Designations,

extensions, terminations and other documents regarding TPS are published in the **Federal Register**. Currently, nationals of Somalia, Sudan, Burundi, Honduras, Nicaragua, and El Salvador have TPS status in the United States.

In many cases, TPS status for a particular country will remain in place for several years. Thus, nationals of these countries may be in the United States for a decade or more and establish a record that TSA can effectively review for a security threat assessment. Based on this and the unrestricted work authorization, we have determined that under certain circumstances, TPS recipients should be permitted to hold a TWIC. Our ability to complete a thorough threat assessment and the record that is disclosed during the threat assessment will be critical factors in determining if a waiver should be granted to a TPS recipient. In addition, letters of reference from employers, teachers, and religious or spiritual personnel are also important to reach a determination on a waiver. Part 1515 lists the information TSA reviews in making waiver determinations, which now also apply to TPS recipients.

Finally, on October 17, 2006 Congress passed the John Warner National Defense Authorization Act for Fiscal Year 2007 (P.L. 109-364). In that Act, Congress amended 46 U.S.C. 8103 to permit an alien allowed to be employed in the U.S. under the Immigration and Nationality Act who meets additional requirements for service as a steward aboard large passenger vessels to obtain an MMD. Since all MMD holders must obtain a TWIC, we have extended this statutory requirement to TWIC as well. Individuals who would satisfy the statutory requirements would most likely, if not always, possess a C-1/D Crewman Visa. The C-1/D visa has been added to the list of acceptable restricted nonimmigrant visas.

Table 2 indicates the types of visas that a lawful nonimmigrant with a restricted visa must hold in order to demonstrate eligibility to apply for a TWIC.

TABLE 2.—TYPES OF VISAS THAT A NONIMMIGRANT WITH A RESTRICTED VISA MUST HOLD

Visa	Nonimmigrant classifications	Description/information
C-1/D	Combined Transit and Crewman Visa. 8 CFR 214.2(c)(D)	For alien crewmen serving in good faith in a capacity required for normal operation and service on board a vessel who intends to land temporarily and solely in pursuit of his calling as a vessel crewman.
E-1	Treaty Trader (see 8 CFR 214.2(e)(1)).	For nationals of a country with which the United States maintains a treaty of commerce and navigation who is coming to the United States to carry on substantial trade, including trade in services or technology, principally between the United States and the treaty country, or to develop and direct the operations of an enterprise in which the national has invested. The employee must intend to depart the United States upon the expiration or termination of E-1 status.

TABLE 2.—TYPES OF VISAS THAT A NONIMMIGRANT WITH A RESTRICTED VISA MUST HOLD—Continued

Visa	Nonimmigrant classifications	Description/information
E-2	Treaty Investor (see 8 CFR 214.2(e)(2)).	An alien employee of a treaty investor, if otherwise admissible, may be classified as E-2 if the employee is in or is coming to the United States to engage in duties of an executive or supervisory character, or, if employed in a lesser capacity, the employee has special qualifications that make the alien's services essential to the efficient operation of the enterprise. The employee must have the same nationality as the principal alien employer. In addition, the employee must intend to depart the United States upon the expiration or termination of E-2 status.
E-3	Australian in Specialty Occupation.	The E-3 is a new visa category only for Australians coming to the U.S. to work temporarily in a specialty occupation.
H-1B	Specialty Occupations (see 8 CFR 214.2(h)(4)).	Persons who will perform services in a specialty occupation which requires theoretical and practical application of a body of highly specialized knowledge and attainment of a baccalaureate or higher degree or its equivalent (in the specialty) as a minimum requirement for entry into the occupation in the US.
H-1B1	Free Trade Agreement (FTA) Professional Visa (H-1B1).	Foreign nationals of countries which have Free Trade Agreements with the United States and are engaged in a specialty occupation are eligible for the H-1B1 FTA Professional Visa [Free Trade Agreement (FTA) Professional Visa]. A U.S. employer must furnish a job letter specifying the details of the temporary position (including job responsibilities, salary and benefits, duration, description of the employing company, qualifications of the applicant) and confirming the employment offer.
L-1	Executive, managerial	An alien who within the preceding three years has been employed abroad for one continuous year by a qualifying organization may be admitted temporarily to the United States to be employed by a parent, branch, affiliate, or subsidiary of that employer in a managerial or executive capacity, or in a position requiring specialized knowledge.
O-1	Extraordinary Ability or Achievement.	An alien who has extraordinary ability in the sciences, arts, education, or athletics, which has been demonstrated by sustained national or international achievement.
TN	North American Free Trade Agreement (NAFTA) visas for Canadians and Mexicans.	The nonimmigrant NAFTA Professional (TN) visa allows citizens of Canada and Mexico, as NAFTA professionals, to work in the United States.
M-1	Vocational student	This visa category is for a fixed time needed to complete the course of study and training. For purposes of the final rule, only students who are attending the U.S. Merchant Marine Academy or comparable State maritime school and hold this visa are permitted to apply for a TWIC.

We are making an additional change to the application information required of TWIC applicants who are not U.S. nationals. In 49 CFR 1572.17, we are requiring all aliens to bring to enrollment the documents that verify the immigration status they are in as of the date of enrollment. We will examine the documents to ensure that the applicant is eligible to apply for a TWIC under the immigration standards and then scan the documents into the TSA system so that they become part of the enrollment record.

In addition, we are requiring drivers with commercial licenses from Canada to provide a Canadian passport at enrollment, if they do not hold a Free and Secure Trade (FAST) card⁶. We know that Canadian TWIC applicants who hold a FAST card have completed a thorough background check by the Canadian government. However, Canadian provinces do not always

require Canadian citizenship or in some cases, lawful presence, when issuing a drivers license. Therefore, we do not believe it is advisable to issue a TWIC based solely on a Canadian driver's license. We are not requiring this of Mexican-licensed drivers who apply for a TWIC because they must obtain border crossing documents to enter the United States, which are issued after the Mexican government has completed a review of the individual and determined they are Mexican citizens or are lawfully present in Mexico.

(e). Mental Incapacity

TSA is changing the waiver process to permit applicants who in the past have been involuntarily committed to a mental health facility or declared mentally incapable of handling their affairs to apply for a waiver without always having to provide documentation showing that the disqualifying condition is no longer present, as we have previously. For example, there may be cases in which an individual has an addiction to drugs or alcohol and is involuntarily committed to a mental health facility to complete rehabilitation. If the individual wishes to apply for a waiver, documents showing that applicant

completed rehabilitation successfully would be critical to TSA's determination on the waiver request. The individual may no longer use illegal drugs or drink alcohol, but technically they may still have an addiction. Therefore, we believe TSA should decide these waiver requests on a case-by-case basis. The documentation submitted to TSA in support of the waiver request will be very important in making the waiver determination. Applicants and/or their representatives should carefully consider and include all available information TSA can use to determine if the applicant poses a security threat.

(f). Fees

Section 520 of the 2004 DHS Appropriations Act, Pub. L. 108-90, requires TSA to collect reasonable fees for providing credentialing and background investigations in the field of transportation. Fees may be collected to pay for the costs of: (1) Conducting or obtaining a CHRC; (2) reviewing available law enforcement databases, commercial databases, and records of other governmental and international agencies; (3) reviewing and adjudicating requests for waivers and appeals of TSA decisions; and (4) other costs related to

⁶ The FAST program is a cooperative effort between the Bureau of Customs and Border Patrol (CBP) and the governments of Canada and Mexico to coordinate processes for the clearance of commercial shipments at the U.S.-Canada and U.S.-Mexico borders. Participants in the FAST program, which requires successful completion of a background records check, may receive expedited entrance privileges at the northern and southern borders.

performing the security threat assessment or the background records check, or providing the credential. Section 520 requires that any fee collected must be available only to pay for the costs incurred in providing services in connection with performing the security threat assessment, or the background records check, or providing the credential. The funds generated by the fee do not have a limited period of time in which they must be used. They can be used until they are fully spent. TSA has also established the fees in this final rule pursuant to the requirements of the General User Fee Statute (31 U.S.C. 9701), which requires fees to be fair and based on: (1) Costs to the government; (2) the value of the service or thing to the recipient; (3) public policy or interest served; and (4) other relevant facts.

In this final rule, TSA uses slightly different terminology to describe the three types of fees and their segments than was used in the NPRM. The Standard TWIC Fee is the fee that an applicant would pay to obtain or renew a TWIC. The Standard TWIC Fee contains the following segments:

- Enrollment Segment (referred to as the “Information Collection/Credential Issuance Fee” in the NPRM),

- Full Card Production/Security Threat Assessment (STA) Segment (referred to as the “Threat Assessment/Credential Production Fee” in the NPRM), and

- FBI Segment (referred to as the “FBI Fee” in the NPRM).

The Reduced TWIC Fee is the fee an applicant would pay to obtain a TWIC when the applicant has undergone a comparable threat assessment in connection with an HME, a FAST card, or other threat assessment, as provided in § 1572.5(e), or holds an MMD or License as provided in § 1572.19(b). The Reduced TWIC fee is made up of the following segments:

- Enrollment Segment, and
- Reduced Card Production/STA Segment (referred to as the “reduced fee for the Security Threat Assessment/Credential Production Fee” in the NPRM).

The Card Replacement Fee is the fee that an applicant would pay to replace a credential that has been lost, stolen, or damaged and is made up of the Card Replacement Segment.

In the TWIC NPRM, TSA proposed to set the Standard TWIC Fee at \$129–149, including the Enrollment Segment of \$45–65, the Full Card Production/Security Threat Assessment (STA) Segment of \$62, and the FBI Segment of

\$22. TSA proposed that the Reduced TWIC Fee be set at \$95–115, including the Enrollment Segment of \$45–65 and the Reduced Card Production/STA Segment of \$50.⁷ TSA proposed that the Card Replacement Fee, composed of the Card Replacement Segment, be set at \$36. *See* 71 FR at 29405, 29428–29431.

In this final rule, TSA establishes the Standard TWIC Fee at \$139–159, including the Enrollment Segment of \$45–65, the Full Card Production/STA Segment of \$72, and the FBI Segment of \$22.⁸ The total Reduced TWIC Fee is set at \$107–127, including the Enrollment Segment of \$45–53 and the Reduced Card Production/STA Segment of \$62.

In this final rule, TSA establishes the Replacement Card Fee of \$36, as was in the NPRM. TSA’s analysis shows that this fee is costed out at \$60, but is not including that amount in the final rule due to the large difference in amount from the NPRM. TSA proposes in this final rule to change the Replacement Card Fee to \$60 based on the reevaluation of costs elements discussed below, and requests comments only on this fee. *See* Request for Comments in Section VI.

Table 3 compares the NPRM per person fee and segments amounts to the final rule per person fee and segments amounts:

TABLE 3.—TWIC PER PERSON FEE SEGMENTS—NPRM VS. FINAL RULE

	NPRM	Final rule	\$ Increase	% Increase
Standard TWIC Fee				
Enrollment Segment	\$45–\$65	\$45–\$65		
Full Card Production/STA Segment (for Individuals requiring a full STA)	62	72	\$10	
FBI Segment:	22	22		
Total	129–149	139–159	10	7.86–6.7
Reduced TWIC Fee				
Enrollment Segment	45–65	45–65		
Reduced Card Production/STA Segment (for Individuals not requiring a full STA):	50	62	12	
Total	95–115	107–127	12	12.6–10.4
Card Replacement Fee				
Card Replacement Segment	36	60 ⁹	24	66.7

No applicant will be required to pay a fee until after TSA publishes this notice in the **Federal Register**.

Cost Components

The NPRM identified the cost components from which the proposed fees were calculated. These are the same

components that were used to calculate the final fees. However, the fees themselves have changed for the reasons described in this section. Since publication of the NPRM, the TWIC program has reevaluated the cost estimates that drive the TWIC fees.

Table 4 lists the cost components of the TWIC Program as estimated for the NPRM and compares them to the costs estimated for the final rule. These cost components are used to derive the TWIC fees that must be collected to fully recover program costs.

⁷ While the proposed rule text at § 1572.503(2) indicated that the Reduced TWIC Fee included both the Enrollment Segment and the Reduced Card Production/STA Segment, it erroneously listed the

fee at \$50. The total for this fee was correctly stated in the preamble as \$95. *See* 98 FR at 29045.

⁸ If the FBI changes its fee in the future, TSA will collect the amended fee.

⁹ While this rule sets a Card Replacement Fee of \$36, TSA is proposing that the Card Replacement Fee be increased to \$60 and is seeking comment only on the Card Replacement Fee. *See* Request for Comments Section VI.

TABLE 4.—5-YEAR TOTAL TWIC COST COMPONENTS—NPRM VS. FINAL RULE

Cost components	NPRM	Final rule	Percent change	Standard TWIC fee	Reduced TWIC fee	Card replacement fee
Enrollment/Issuance	\$65,212,285	\$65,980,199	1	X	X	X ¹⁰
Threat Assessments ¹¹	42,463,118	32,120,927	-24	X	X ¹²
IDMS	18,783,000	44,190,882	135	X	X	X
Card Production	20,427,000	28,346,657	39	X	X	X
Program Support	22,641,000	18,810,786	-17	X	X	X
Total	169,526,403	189,449,451	12			

As shown by Table 4, some of the cost components decreased from the NPRM costs estimates, while some increased. The Enrollment/Issuance cost component increased by approximately 1 percent due to further analysis that indicated a need to account for the contractor fee associated with replacing a lost, stolen, or damaged card. This contractor fee is estimated at \$5. This card re-issuance cost within the Card Replacement Fee was not included as part of the NPRM estimate.

The Threat Assessments cost component decreased overall by approximately 24 percent. While the costs associated with adjudication by ALJs have been added, cost reductions for perpetual vetting and threat assessment gateway account for the overall reduction.

The IDMS cost component increased based on a re-evaluation of the overall IDMS costs. The program office identified: (1) The need to increase the hardware and software required to obtain a Security Certification & Accreditation, and to support the full volume of TWIC applicants; (2) system changes required to address security vulnerabilities; and (3) increases in contractor support necessary for systems operations and maintenance. The total increase is estimated at \$19 per credential produced.

The Card Production cost increased by approximately 39 percent based on two factors. First, in order to produce cards more rapidly during the initial

enrollment, additional shifts were required at the card production facility. This decision was made in order to address comments to the NPRM that cards needed to be produced as quickly as possible. Second, TSA and Coast Guard received comments to the NPRM on the need to support contactless biometric authentication based on the harsh conditions of the maritime environment and operational efficiencies. In order to address these comments TSA and the Coast Guard have established a NMSAC working group to recommend a contactless TWIC technology specification. Second, we have added a fee to cover future technology-related product improvements to the TWIC system and credential. Technology improvements occur rapidly and in order to take advantage of the efficiency these improvements provide, we must plan for that cost. Building in the cost of technology and system improvements is a common practice for programs that rely so heavily on software and hardware to collect and transmit large amounts of information.

The Program Support cost decreased by approximately 17 percent because the program office reevaluated and decreased program staffing levels required to support the maritime population after the initial maritime enrollment period. Additionally, Program Support costs related to interagency communication requirements also decreased. These cost reductions resulted in approximately a \$2 per card decrease.

The discussion below describes the cost components associated with each type of fee, Standard, Reduced and Card Replacement. Although the overall program costs increased by approximately 12 percent, the three types of TWIC fees did not increase by 12 percent as each fee is composed of different cost components.

The per person cost segments for the Standard TWIC Fee are derived from all five of the cost components in the Total TWIC Cost Components table above—Enrollment/Issuance, Threat

Assessments,¹³ IDMS, Card Production, and Program Support. Note that the IDMS, Card Production, Program Support cost components makeup the Card Production/STA and FBI segments of the Standard and Reduced TWIC Fees. The net increase in the total for the Standard TWIC Fee is based primarily on the increase of the IDMS and Card Production cost components, as described above in the analysis of the TWIC cost components.

The per person cost segments for the Reduced TWIC Fee are also derived from five of the cost components in the Total TWIC Cost Components Table 4—Enrollment/Issuance, Threat Assessments,¹⁴ IDMS, Card Production, and Program Support. The net increase in the Reduced TWIC Fee is based on the reevaluation of the cost components, as described in the analysis of the TWIC cost components above. It should be noted that the reduced fee does not include the entire Threat Assessments cost component. Because the Reduced TWIC Fee does not include this entire cost component, this fee does not entirely benefit from the reduction in the Threat Assessments cost component, and therefore, increased at a greater percentage than the Standard TWIC Fee.

The per person cost for the Card Replacement Fee is derived from four of the cost components in the Total TWIC Cost Components Table 4—Enrollment/Issuance,¹⁵ IDMS, Card Production, and Program Support. The net increase in the Card Replacement Fee of \$24 is based on the reevaluation of the cost components, as described in the analysis of TWIC cost components

¹⁰ While the majority of the Enrollment/Issuance requirements have already been satisfied by the applicant through initial enrollment, there are still some enrollment/issuance functions associated with these card replacements, such as overhead. Therefore, these applicants will not be burdened with the normal enrollment/issuance cost component.

¹¹ The Threat Assessments, IDMS, Card Production and Program Support Components makeup the Card Production/STA and the FBI Segments.

¹² While the majority of the Threat Assessment requirements have already been satisfied by the applicant through participation in a previous security fee, there are still some threat assessment functions associated with these applicants, such as CSOC activities. Therefore, these applicants will pay the Reduced Card Productions/STA Segment.

¹³ The Threat Assessment cost component includes the FBI Segment of the Standard TWIC Fee.

¹⁴ As stated in footnote 11, although the majority of the Threat Assessment requirements have already been satisfied by the applicant through participation in a previous security fee, there are still some threat assessment functions associated with these applicants.

¹⁵ As stated in footnote 10, although the majority of the Enrollment/Issuance requirements have already been satisfied by the applicant through initial enrollment, there are still some enrollment/issuance functions associated with these card replacements, such as overhead.

above. It should be noted that this fee does not include the entire Enrollment/ Issuance cost component or any of the Threat Assessments cost component. Because this fee does not include the Threat Assessments cost component, this fee does not benefit from the reduction in the Threat Assessments cost component. Thus, the Card Replacement Fee has increased at a greater percentage than the Standard and Reduced TWIC Fees. Because this fee is substantially higher than that in the NPRM, TSA is establishing \$36 as the fee in this rule but is proposing to increase the fee to \$60 and is providing the public an opportunity to submit additional comments on the card replacement fee. *See* Request for Comments in Section VI.

An Additional Notice on Fees

As Table 3 indicates, the Enrollment Segment is a range of \$45–\$65 for both the NPRM and the final rule. TSA is unable to finalize the fee because we do not yet have a final contract with an enrollment provider. When a final contract is executed, TSA will publish a Notice in the **Federal Register** that will specify the amount for that segment and all of the fees. Therefore, the rule text does not contain TSA's exact fee numbers, but it does include the FBI fee. No applicant will be required to pay a fee until after TSA publishes this notice in the **Federal Register**.

(g). Drivers Licensed in Mexico and Canada Transporting Hazardous Materials

In accordance with sec. 7105 of SAFETEA–LU, commercial motor vehicle drivers licensed in Canada or Mexico may not transport hazardous materials into or within the United States unless they undergo a background check that is similar to that undergone by U.S.-licensed drivers.¹⁶ TSA has determined that a card issued by the Bureau of Customs and Border Protection (CBP) under the FAST program provides a similar background check. *See* 71 FR 44874 (August 7, 2006). The security threat assessment that is required under this final rule for issuance of a TWIC is the same background check currently required for U.S.-licensed drivers with HMEs. Therefore, we are amending 49 CFR 1572.201 to allow possession of a TWIC card by a driver licensed in Mexico or Canada to satisfy the SAFETEA–LU requirement. Thus, drivers licensed in Canada or Mexico may obtain either a FAST card or a TWIC to meet the requirement that they have a

background check that is similar to that of a U.S. hazmat driver.

In this final rule, for administrative purposes, we are reprinting the entire part 1572. We are making only a couple of changes to § 1572.203, however. We are changing its title to more clearly reflect its scope, to “Transportation of explosives from Canada to the United States via railroad carrier.” In § 1572.203(b) we are changing the definition of “Customs Service” to “Customs and Border Protection (CBP)” to reflect the reorganization of the U.S. Customs Service under the Homeland Security Act of 2002.

(h). Compliance and Enforcement Matters

We are adding a new section. (49 CFR 1570.7) to make it clear that it is a violation of this rule, and other applicable federal laws, to circumvent or tamper with the access control procedures. This section also clarifies that it is a violation for any person to use or attempt to use a credential that was issued to, or a security threat assessment conducted for, another person. In addition, no person may make, cause to be made, use, or cause to use, a false or fraudulently-created TWIC or security threat assessment issued or conducted under this subchapter. Finally, it is a violation of this rule, and other applicable federal laws, for any person to cause or attempt to cause another person to violate these procedures. Violations of any provision of this rule may be subject to such civil, criminal or administrative actions as are authorized under federal law.

Note that the acts identified in § 1570.7 may also be violations of Federal criminal law, such as 18 U.S.C. 701 (Official badges, identification cards, other insignia), 18 U.S.C. 1001 (Statements or entries generally), 18 U.S.C. 1028 (Fraud and related activity in connection with identification documents and information), 18 U.S.C. 1029 (Fraud and related activity in connection with access devices). In appropriate cases, TSA will refer to the Department of Justice (DOJ) matters for criminal investigation and, if appropriate, criminal prosecution.

Section 1570.9 is being added to make clear that a person must allow his or her TWIC to be inspected upon request of an appropriate official. For clarification purposes, Coast Guard has provided a similar requirement in 33 CFR 101.515(d) adopting the same language as § 1570.9.

As discussed in section C.4. of this preamble, § 1570.11, Compliance, inspection, and enforcement, was proposed in the NPRM as § 1572.41.

D. Anticipated Future Notices and Rulemaking

1. Notices

We will publish several notices in the **Federal Register** to facilitate implementation of the TWIC program. Specifically, a notice will be published:

- (a) establishing the fees for the TWIC, as stated above in C.2(f);
- (b) for each COTP zone, prior to beginning the enrollment period; and
- (c) for each COTP zone, 90-days prior to requiring compliance with these regulations.

2. Rulemaking

In the future we will issue another NPRM to propose card reader requirements for MTSA-regulated vessels and facilities. It will be issued with a comment period that is long enough for all interested persons to reasonably be able to provide comment, and it will announce public meetings in a variety of places. We cannot, at this time, make any definitive statement on where those places will be, but we will consider the locations suggested by commenters and inform the public of upcoming meeting information in advance in the **Federal Register**.

E. Summary of TWIC Process Under the Final Rule

The TWIC program was developed to improve identity management and credentialing shortcomings that exist in segments of the transportation industry. TSA evaluated a variety of technologies, used field testing, and to the extent possible, incorporated the basic tenets of Homeland Security Presidential Directive 12 (HSPD–12)¹⁷ to arrive at the credential and enrollment process implemented in this program. The standards for the program are to ensure that the credentialing processes: (1) Are administered by accredited providers; (2) are based on sound criteria for verifying an individual's identity; (3) include a credential that is resistant to fraud, tampering, counterfeiting and terrorist exploitation; and (4) ensure that the credential can be quickly and electronically authenticated.

The purpose of the TWIC program is to ensure that only authorized personnel who have successfully completed a security threat assessment have unescorted access to secure areas of maritime facilities and vessels. The credential will include a reference biometric that securely links the credential holder to the issued

¹⁷ HSPD–12 requires Federal agencies and their contractors to adopt an identity management and credentialing system that uses biometrics.

¹⁶ 49 U.S.C. 5103a(h).

credential. At any time, TWIC holders may be asked to confirm that they are the rightful owner of the credential by matching their biometric to the one stored on the credential. An individual's credential is revoked by TSA if disqualifying information is discovered or the credential is lost, damaged or stolen. When a credential is revoked, TSA lists it on the list of revoked cards, or 'hotlist' by the unique serial number assigned to the credential. Therefore, a revoked credential that is compared against the hotlist will be flagged and access would not be granted.

TSA has designed the TWIC process to maintain strict privacy controls so that a holder's biographic and biometric information cannot be compromised. The TWIC process implemented in this rule is described below from the perspective of an applicant.

1. Pre-Enrollment and Enrollment

TWIC enrollment will be conducted by TSA or TSA's agent operating under TSA's direction. These personnel are known as Trusted Agents. All Trusted Agents must successfully complete a TSA security threat assessment and receive extensive training before they are authorized to access documents, systems, or secure areas.

DHS will publish a notice in the **Federal Register** indicating when enrollment at a specific location will begin and when it is expected to terminate. Once DHS has published that notice, facility and vessel owners/operators (owners/operators) must notify workers of their responsibility to enroll into the TWIC program during the enrollment period. Regarding the compliance date for facilities, DHS will also publish this information in the **Federal Register** for each COTP zone at least 90-days in advance. Owners and operators are required to inform their employees of this date as well. (The implementation plan for enrollment is discussed in greater detail below.) TSA and the Coast Guard will work with owners/operators to ensure that they can provide applicants sufficient time to enroll, complete the security threat assessment and any necessary appeal or waiver process, and obtain the credential before the applicant is required to present the credential for access to a facility or vessel. As TWIC is implemented, owners/operators must give individuals at least 60 days notice to begin the enrollment process. Generally, TSA completes a threat assessment in approximately 10 days when there is no indication that the applicant may not meet the TWIC enrollment criteria. If criminal activity or other potentially disqualifying

information is revealed, however, TSA cannot guarantee that such information will be favorably resolved and a threat assessment completed in less than 30 days.

Applicants are encouraged to "pre-enroll" online to reduce the time needed to complete the entire enrollment process at an enrollment center. The convenience of pre-enrollment is a significant benefit for applicants and reduces strain on the enrollment centers. The pre-enrollment process allows applicants to provide much of the biographic information required for enrollment and to select an enrollment center where they wish to complete enrollment. While pre-enrolling, applicants may schedule an appointment to complete enrollment at an enrollment center, although appointments are not required at enrollment centers. For pre-enrollment, applicants may use a personal computer with access to the internet or they may use TWIC kiosks. The TWIC kiosks will be set up by the TSA agent when enrollment begins at locations convenient to the affected population, including enrollment centers, and are similar to an ATM machine.

The Web address for pre-enrollment and all additional information relating to the TWIC program is www.tsa.gov/twic. The TWIC Web site also will list the documents the applicant must bring to the enrollment center to verify identity so that all applicants can be properly prepared. Mariners who must prove U.S. citizenship or immigration status to obtain an MMD, license, COR, STCW endorsement or MMC must provide the documents required by the Coast Guard at 46 CFR chapter I, subchapter B at the time of enrollment.¹⁸ TSA will scan these documents into the enrollment record, which will be forwarded to the Coast Guard. In addition, applicants who are not U.S. citizens or nationals must bring their immigration documents, including visas and naturalization paperwork, to enrollment so that the documents which prove legal presence in the United States can be scanned into the enrollment record.

¹⁸ In order to allow the Coast Guard to remove the requirement that all mariners apply for their credentials in person at a Regional Examination Center (REC), it is necessary for TSA to document proof of citizenship, as the citizenship requirements for certain Coast Guard-issued mariner credentials are stricter than the overall TWIC citizenship requirements. For more information on mariner credentials and the Coast Guard's plan to remove the physical appearance at an REC requirement, see the Coast Guard SNPRM titled "Consolidation of Merchant Mariner Qualification Credentials" published elsewhere in today's **Federal Register**.

At the enrollment center, applicants who pre-enroll must provide documents to verify their identity, confirm that the information provided during pre-enrollment is correct, submit biometrics identifiers, and sign the enrollment documents. At the enrollment center, all applicants will receive a privacy notice and consent form, by which they agree to provide personal information for the security threat assessment and credential. (For applicants who pre-enroll, the privacy notice is provided with the application on-line, but the applicant must acknowledge receipt of the notice in writing at the enrollment center.) If an applicant fails to sign the consent form or does not have the required documents to authenticate identity, enrollment will not proceed.

All information collected at the enrollment center or during the pre-enrollment process, including the signed privacy consent form and identity documents, is scanned into the TSA system for storage. All information is encrypted or stored using methods that protect the information from unauthorized retrieval or use. If an enrollment center temporarily loses its internet connection, the enrollment data is encrypted and stored on the enrollment workstation, but only until an internet connection is restored.

Applicants will provide fingerprints from each hand and sit for a digital photograph. We will collect a print from all 10 fingers unless the applicant has lost or seriously injured his or her fingers. TSA will provide alternative procedures for enrollment centers to use if an applicant cannot provide any fingerprints. The fingerprints and photograph will be electronically captured at the enrollment center and made part of the applicant's TWIC enrollment record. The fingerprint images collected from each applicant will be submitted to the FBI for the CHRC.

The TWIC fee, which covers the cost of enrollment, threat assessment, and credential production and delivery, will be collected from the applicant at the enrollment center. Payment can be made by cashier's check, money order, or credit card. The TWIC enrollment fee is non-refundable, even if the threat assessment results in denying a TWIC to the applicant.

The entire enrollment record (including all fingerprints collected) will be transmitted to the TSA system, encrypted, and segmented to prevent unauthorized use. The TSA system acknowledges receipt of the enrollment record, at which time all enrollment data is automatically deleted from the enrollment workstation. At this point,

enrollment data is stored only in the TSA system, and is stored there as encrypted data. The TSA system contains many feedback mechanisms to validate the transmission and receipt of data at key points in the process. The status of each transmission is recorded within the system.

As discussed in the TWIC NPRM (71 FR 29402), during TSA's Prototype testing phase of the program, the average time needed for an applicant who pre-enrolled to complete enrollment was 10 minutes, 21 seconds. TSA expects that it will take approximately fifteen minutes to complete enrollment of applicants who do not pre-enroll.

TSA and Coast Guard plan to use a phased enrollment approach based on risk assessment and cost/benefit analysis to implement the program nationwide. Locations that are considered critical and provide the greatest number of individual applicants will be among the earliest enrollment sites. As stated above, TSA will publish a notice in the **Federal Register** indicating when enrollment at a specific location will begin and when it is expected to terminate. In addition, DHS will publish a notice in the **Federal Register** indicating the compliance date for each COTP zone. This notice will be published at least 90 days prior to the compliance date. There are approximately 130 locations where TSA plans to enroll applicants. TSA and Coast Guard will work closely with the maritime industry to ensure that owners/operators and workers are given as much notice as possible of the commencement of enrollment at their location. (See the discussion of § 1572.19 below for additional information on the timing of enrollment.) TSA will use a combination of fixed and mobile enrollment stations to make the enrollment process as efficient as possible for applicants and owners/operators.

2. Adjudication of Security Threat Assessment

Following enrollment, the TSA system sends pertinent parts of the record to various sources so that appropriate terrorist threat, criminal history, and immigration checks can be performed. When the checks are completed, TSA makes a determination whether to issue a TWIC to the applicant and notifies the applicant of that decision. If the applicant is deemed to be qualified, the TSA system notifies the credential production portion of the system to create a credential. TSA sends the applicant a Determination of No

Security Threat via U.S. mail, and the TSA system notifies the applicant when the credential is ready to be retrieved from the enrollment center. Notifications from the TSA system that a credential is ready for pick-up will be through e-mail or voice mail, depending on the preference the applicant expresses on the application.

If TSA determines that the applicant is not qualified, TSA sends an Initial Determination of Threat Assessment to the applicant via U.S. mail, with information concerning the nature of the disqualification, and how the applicant may appeal the determination or apply for a waiver of the standards. If the applicant proceeds with an appeal or application for waiver that is successful, TSA will notify the applicant accordingly and the credential production process begins. (The appeal and waiver processes are discussed in greater detail below in the discussion of 49 CFR part 1515.)

3. Credential Production and Delivery

If the applicant is deemed by TSA to be qualified to receive a TWIC, the TSA system generates an order to produce a credential. The TWIC is produced at a government credential production facility. The face of the TWIC credential contains the applicant's photograph, name, TWIC expiration date, and a unique credential number. In addition, the credential will store a reference biometric, a personal identification number (PIN) selected by the applicant, a digital facial image, an expiration date, and a Federal Agency Smart Credential number. The PIN can subsequently be used as an additional security factor in authenticating identity and authorizing use of the credential; or it can be used as the primary verification tool if the biometric is inoperative for some reason.

4. Receiving the Credential

The TSA system will notify the applicant when the credential is ready, and what if any additional steps the applicant must take to receive the credential. Once the enrollment and issuance process is completed, the credential is activated and is ready to be presented at a facility or vessel for use as an access control tool. The TWIC security threat assessment and credential are valid for five years, unless information is discovered that causes TSA to revoke the credential.

5. Lost, Damaged, or Stolen TWICs

Replacement TWICs are available if a credential is lost, stolen, or damaged. As soon as a TWIC holder becomes aware that his credential is missing or

damaged, he must report this fact by calling the TWIC Call Center which will be open 24 hours per day, 7 days a week. TSA will post the Call Center number on the TWIC web site as soon as it is available, and it will be posted at all enrollment centers and kiosks. The Center follows a standard process to revoke the credential, and order printing and transmission of a replacement. TSA adds the lost, damaged or stolen credential to the 'hotlist,' which includes the Smart Card number of all credentials that TSA has revoked. Applicants must pay a fee of \$36¹⁹ to cover the cost of invalidating the previous credential, production of a replacement credential, shipping, and other appropriate program costs. The reissued TWIC will have the same expiration date as the lost/damaged/stolen TWIC.

6. Renewal

TWICs issued under this rule remain valid for a period of five years, unless renewed before the five-year term ends. Upon renewal, an applicant receives a new credential and the old credential is invalidated in the TSA System. TSA does not plan to notify TWIC holders when their credential is about to expire because the expiration date will be displayed on the face of the credential. To renew a TWIC, the holder must appear at any enrollment center, at least 30 days before expiration, to initiate the renewal process. This will provide sufficient time for TSA to conduct the security threat assessment and the Coast Guard to complete any review necessary to renew any required mariner documents. During renewal, applicants must provide the same biographic and biometric information and identity verification documents required in the initial enrollment and pay the associated fees. Note that the TWIC web site will maintain a list of documents that may be used to verify identity, which may change over time. A new credential is issued upon renewal using the same issuance process as used in the initial TWIC issuance and the expired credential will be invalidated. The newly issued credential will have an expiration date five years from the date of issuance of the new credential. Although renewal only occurs every five years, TSA conducts recurring checks on individuals throughout the five year period, so that newly-discovered information informs the access rights of individuals.

¹⁹ We request comments on changes to the card replacement fee in Section VI below.

7. Call Center

Toll-free TWIC Call Center (Help Desk) support will provide around-the-clock service for transportation workers, facility operators, and others who require assistance. Assistance includes help for pre-enrollment; enrollment; and lost, stolen, or damaged card reporting and replacement. Help will also be available for scheduling enrollment appointments, locating the closest enrollment facility to an applicant, guiding applicants through the Web-based pre-enrollment process, and for checking on the status of a TWIC application.

F. SAFE Port Act of 2006

On October 13, 2006, the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347) was enacted. The portions of the Act which relate to the TWIC program are discussed below.

Section 104(a) of the SAFE Port Act contains a number of amendments to the basic requirement in MTSA for credentialing codified in 46 U.S.C. 70105. New sec. 70105(g) mandates concurrent processing by TSA and the Coast Guard of an individual's application for an MMD²⁰ and a TWIC. This final rule is in compliance with this requirement. TSA will share with the Coast Guard the individual's CHRC, fingerprints, photograph and proofs of citizenship and identity, which will allow the Coast Guard to begin evaluating whether the individual is qualified to obtain an MMD while TSA completes its security threat assessment. TSA will also share the results of their security threat assessment with the Coast Guard to ensure that MMDs are only issued to individuals who pass the security threat assessment and are issued a TWIC. Thus, such applicants will only submit one set of fingerprints and other information relating to citizenship, alien status, and criminal history, which will be used by both TSA and the Coast Guard.

New sec. 70105(h) requires that applicants who have passed a security threat assessment for an HME or MMD pay only for the costs associated with the issuance, production, and management of the TWIC and are not charged for the cost of another threat assessment. This final rule is in compliance with this requirement in that TSA will not charge those who

already hold an HME or MMD for an additional threat assessment under TWIC. Rather, TSA will charge a reduced fee.

New sec. 70105(i) provides requirements for implementing TWIC across the nation by prioritizing the ports based on risk, and requires that the TWIC program is to be implemented according to the following schedule: (1) top ten priority ports by July 1, 2007; (2) the next forty priority ports by January 1, 2008; and (3) all other ports by January 1, 2009. Under new sec. 70105(j) each application for a TWIC made by someone holding an MMD as of the date of enactment of this bill must be processed by January 1, 2009. We are now planning how to meet these requirements and will establish the implementation schedule accordingly.

New sec. 70105(k) requires DHS to conduct a pilot program on card readers as set out in that section. DHS is currently analyzing how best to meet these requirements, and will begin the pilot program as soon as practicable.

Under new sec. 70105(m) DHS may not require card readers to be placed aboard a ship unless the crew's number is in excess of the number determined to require a reader or if the Secretary determines that the vessel is at risk of a severe transportation security incident. When DHS drafts the rule that will require use of card readers by vessel owners and operators, it will do so in compliance with this requirement.

SAFE Port Act sec. 104(b) has additional amendments to MTSA. It revises 46 U.S.C. 70105(b) by adding a paragraph making clear the Secretary has the discretion to add to the list of those individuals who otherwise may be required to obtain a TWIC. The Secretary may apply TWIC requirements to individuals including those "not otherwise covered by this subsection". TSA has exercised this discretion by allowing Canadian and Mexican commercial drivers who transport hazardous materials to obtain TWICs, which will allow them to transport hazardous materials in the United States. Further, SAFE Port Act sec. 104(b) clarifies in sec. 70105(c) that DHS must establish a waiver and appeal process for applicants denied a TWIC under sec. 70105(c)(1)(A) or (B) (criminal history) or (D) (otherwise poses a security threat). TSA's new process in 49 CFR part 1515 complies with this requirement.

Under SAFE Port Act sec. 104(c), the deadline for final TWIC regulations remains January 1, 2007. Further, the regulation must include a provision for an interim check against terrorist watchlist databases so as to enable new

workers to start working immediately. This final rule is in compliance with this requirement. As explained in detail elsewhere in this preamble, owners or operators wishing to put their newly hired direct employees to work immediately, prior to issuance of the new hire's TWIC, may do so provided that the new hire is successfully checked against various terrorist databases. The procedure for running the new hire's information through these checks can be found in 33 CFR 104.267, 105.257, and 106.262.

SAFE Port Act sec. 106 states that applicants convicted of treason, espionage, sedition, and crimes listed in chapter 113B of title 18, U.S.C., or comparable State laws must be disqualified from holding a TWIC. The list of disqualifying crimes in 49 CFR 1572.103 complies with this requirement by including these crimes as disqualifying.

III. Discussion of Comments

TSA and the Coast Guard received approximately 1770 comments on the TWIC NPRM during the 45-day comment period. In addition, an estimated 1200 people attended the four public meetings that were held between May 31 and June 7, 2006. Copies of the written comments received, as well as transcripts of the public meetings, are available to the public on www.regulations.gov at the public docket for this rulemaking action.

Numerous commenters supported the concept and purpose of the TWIC program as a method of protecting national maritime security. Some expressed their support unequivocally. One commenter requested that its port be selected for the first phase of the enrollment and implementation process. Several commenters who generally agreed with the idea of the TWIC, also criticized certain details of the proposal, expressed qualifications of various kinds, or said the proposal needed to be more efficient, workable, and fair. Some terminal operators and marine engineers who supported TWIC said that although it would achieve greater maritime security, they were concerned about its burden on industry or noted that security needed to be balanced against fairness for maritime workers. One commenter who generally supported the implementation of TWIC was concerned about the impact of the proposed rules on the efficiency of port facility operations, and suggested a more phased and flexible approach. Another commenter asked for more of a risk-management approach with a performance-based set of guidelines and a reevaluated technology. An

²⁰ Although the SAFE Port Act only created this requirement for MMDs, TSA and the Coast Guard have also applied concurrent processing, a longer time period to apply for an initial TWIC, and reduced fees to licenses, CORs, STCW endorsements, and the MMC.

association of maritime operators supported security and background checks and digital fingerprint and photographs, but was concerned about the short timeline for implementation, the absence of facilities to provide the necessary services, and the social and economic burden imposed on individuals. Another commenter who supported TWIC thought that the requirements for who must possess a TWIC was over inclusive and that waivers or exemption processes should be added to lower the overall number of people who would require a TWIC. A commenter noted that although employers were responsible for notifying employees of the TWIC requirement, employer sponsorship of the TWIC program was not desirable.

In contrast, many commenters expressed strong general opposition to TWIC without providing explicit reasons. Some said it was unnecessary and unjustified, and would not improve maritime security. Some argued that the rule would be harmful. These commenters cited concerns that TWIC was not the most effective and economic approach, it would adversely affect staffing of vessels and port facilities, and it would cause economic hardship on the industry and individuals. Commenters also stated that TWIC was inappropriate for the inland marine industry, it would harm stevedore/terminal operators, and it was an unnecessary cost and duplication of effort where seaport access credentials are currently in use. One commenter stated that although the current system of licensing and documenting maritime personnel is failing or broken, the addition of TWIC will only add additional delays and burden. One commenter argued that the largest threat existed from foreign vessels, and they should not be excluded. Another commenter found the rule “large-port-centric” and disapproved of this “one-size-fits-all” approach.

TSA’s and Coast Guard’s responses to the comments are discussed below.

A. Requests for Extension of Comment Period and Additional Public Meetings

We received numerous requests to extend the comment period past the 45 days provided in the NPRM. We also received a significant number of comments requesting that we hold additional public meetings. These requests included a large number of supporting reasons.

Several commenters said that TSA and the Coast Guard had not done enough to obtain information about the concerns of affected maritime workers and industries before going forward

with the TWIC rule, and the rule schedule should be extended to allow time for the collection of more information, with public meetings in more sections of the country, such as the Gulf Coast and Great Lakes ports. One commenter said the rule was skewed toward the issues involving large ports. A U.S. Senator argued that more information should have been collected on the impact of the rule on both the inland barge industry and the for-hire passenger excursion boat industry, and an association argued that there was little appreciation of the operational realities of the tugboat, towboat, and barge industry. Another commenter saw little reference to the domestic passenger fleet. Commenters listed the following organizations that they thought should have been consulted: the Passenger Vessel Association, American Waterways Operators Association, the Towing Safety Advisory Committee, the Merchant Personnel Advisory Committee, American Petroleum Institute (API), Offshore Mariner Safety Association (OMSA), and other maritime organizations.

We have carefully considered the comments submitted and nonetheless determined that it is not advisable to extend the comment period, nor did we hold additional public meetings. We considered delaying implementation of this entire project but determined that the security risk associated with such a delay is not acceptable. While the “name checks” being completed by TSA under the Notice published by the Coast Guard on April 28, 2006 (71 FR 25066) do provide some security to the ports, we need the added layer of security that issuing TWICs provides. First, the current name check regime established through the Coast Guard Notice checks names against the terrorist watch lists and immigration databases. With TWIC, we will also check an individual’s criminal history and conduct an enhanced immigration check. Second, the interim vetting regime only applies to permanent employees and long-term contractors of facilities and longshoremen, whereas the TWIC program provides the benefit of performing checks on all individuals with unescorted access to both facilities and vessels. Finally, the TWIC program will provide the owners/operators with the piece that the interim vetting regime is missing—namely, a universal credential to verify whether an individual requesting access to a vessel or facility has been screened and determined not to be a security threat. With the Coast Guard spot checks, we

can also verify, on a random basis, the validity of the TWICs being used to gain entry to vessels and facilities.

As we began reviewing the comments we received at the public meetings and on the docket, we realized that there were some portions of the NPRM that were not ready to be implemented. Most important among these pieces were the card reader and biometric verification requirements. As a result, we have removed those requirements from the final rule. What remains is the requirement to apply for and hold a TWIC, the threat assessment standards to be used when processing TWIC applications, and the reduced access control requirements, where the TWIC is used as a visual identity badge at MTSA-regulated vessels and facilities. The Coast Guard intends to integrate the TWIC requirements into its already existing facility and vessel annual MTSA compliance exams, as well as through unannounced security spot checks to confirm the identity of the TWIC holder using hand-held card readers.

We will initiate a new rulemaking action after pilot testing TWIC readers in the maritime environment. Through that rulemaking action we will propose, seek comment on, and finalize the requirements for card readers. We will also hold public meetings during that rulemaking action, and will consider holding these meetings in any location suggested by commenters. Thus, while we determined that it was not in the public interest to delay implementation of the TWIC program to allow for an extended comment period or additional public meetings, we will be providing an additional opportunity for public participation before owners/operators of vessels and facilities will have to implement the card reader requirements.

B. Coast Guard Provisions

1. Definitions

(a) Requests To Add Additional Definitions

One commenter felt that using the word “ensure” in the regulations establishes an unreasonable standard of care that would require facilities to guarantee safety, and expose facilities to strict liability in the case of a terrorist incident. The commenter recommended that the final rule amend all uses of the word “ensure” in 33 CFR, chapter I, subchapter H.

We disagree. The word ensure, as used in current regulations as well as the TWIC NPRM, was used throughout subchapter H purposely, to designate where the ultimate responsibility for

various security functions would be found for enforcement purposes. We did not propose changing it in the TWIC NPRM and we have not changed it in the final rule.

One commenter recommended that the final rule better define the term "Federal Official" in 33 CFR 101.514, so that active duty and reserve military personnel, all Federal Civil Service employees, and people who hold Department of Defense (DOD) Common Access Card (CAC) cards are not required to obtain or possess a TWIC. We disagree with the suggested change, as the term Federal official is clear enough on its face, meaning individuals who are working for the Federal government. Section 101.514 allows these individuals to gain unescorted access to a vessel or facility using their agency-issued, HSPD-12 compliant identification card. Until an HSPD-12 card is available, these officials may use their agency's official credential—when representing that agency on official duty—if that is the DOD CAC card, then the CAC card may be used.

One commenter noted that a definition for the term "official" is not provided in the proposed rule, and recommended that Federal, State, and local "officials" not requiring a TWIC for unescorted access should be limited to law enforcement, fire, rescue, and government employees that have been subjected to a background screening equivalent to the one conducted for issuance of a TWIC. We believe that the term "official" is clear enough in context, and as such we have not added a definition as suggested by the commenter. We recognize, however, that emergency responders may not fit into the "officials" category, and so we have added a new paragraph to § 101.514 to cover emergency responders during emergency situations.

One commenter recommended that the rule be amended to exclude persons working on vessels whose sole purpose is entertainment, such as musicians on passenger vessels. If this exclusion was not made, the commenter recommended that where a vessel engaged solely in entertainment has been inadvertently grouped with vessels of other classes, that the designation of various spaces aboard the vessels, and within those vessels' facilities, be more clearly defined in the final rule, including: (1) For passenger vessels, exclude the employees, whose workstation is limited to areas accessible by passengers, based on the fact that they are occupying the same areas as the passengers who are not subject to the requirement; and (2) apply the TWIC ruling only to the crew areas or persons

with access to crew areas. This would allow operators to maintain the security of control stations, equipment rooms and voids, without disruption of access to other employee only areas of the vessel or a facility, which do not need to be restricted areas.

We agree with this comment. As discussed above in the section discussing changes to the Coast Guard provisions, we are adding a definition for "employee access areas," for use only by passenger vessels and ferries. An employee access area is a defined space within the access control area of a ferry or passenger vessel that is open to employees but not passengers. It is not a secure area and does not require a TWIC for unescorted access. It may not include any areas defined as restricted areas in the VSP. Note, however, that any employee that needs to have unescorted access to areas of the vessel outside of the passenger or employee access areas will need to obtain a TWIC.

(b). TWIC

Two commenters recommended that all references to a "valid TWIC" be changed to "TWIC" since the definition of TWIC requires that it be valid and non-revoked. We agree and have made the suggested changes within 33 CFR parts 101 through 106. We have left the language in 46 CFR parts 10, 12, and 15, however, because in those places, the term TWIC is not tied to the definition in § 101.105.

(c). Public Access Area/Passenger Access Area

One commenter recommended that the definition of "public access area" for cargo vessels be the same as that for passenger vessels to allow similar flexibility. Alternatively, the commenter provided a separate definition of "public access area" that allows facilities to designate any area as such, provided the area is specified in the FSP.

One association noted that vessels other than "passenger vessels" are permitted to carry passengers, industrial personnel, or persons in addition to the crew. The association recommended that the final rule provide flexibility similar to passenger vessels for other types of vessels by providing the following definition of public access areas in 33 CFR part 101: "Public access areas means those defined spaces within a vessel, facility or OCS facility that do not require a TWIC for unescorted access. Any vessel, facility or OCS facility may designate areas as public access areas provided they are specified in the security plan."

They further recommended that facilities owners and operators be provided flexibility similar to that of passengers in designating public access areas, and recommended that the following definition be added to part 105:

"§ 105.xxx Public access area.

(a) Any facility may designate areas within the facility as public access areas. Any such areas must be specified in the FSP.

(b) Public access areas are those defined spaces within a facility that do not require escorted access for persons not in possession of a TWIC."

They also recommended that OCS facilities owners and operators be provided flexibility similar to that of passenger vessels in designating public access areas, and recommended that the following definition be added to part 106:

"§ 106.xxx Public access area.

(a) Any OCS facility may designate areas within the facility as public access areas. Any such areas must be specified in the FSP.

(b) Public access areas are those defined spaces within an OCS facility that do not require escorted access for persons not in possession of a TWIC."

We disagree with these comments. The concept of a "passenger access area" has been included in the final rule to cover passenger vessels, ferries, and cruise ships, *i.e.*, those vessels that routinely, as part of their normal operating procedures, carry passengers. While we recognize that some cargo vessels may also, at times, carry passengers, we do not feel it is appropriate to expand this provision to other categories of vessels at this time. We feel that appropriate flexibility is given in the interpretation of "escort" to address these situations, while maintaining security. Additionally, facilities are already able to designate certain portions of their facility as "public access areas," therefore we do not feel it necessary to expand the "passenger access area" concept to facilities at this time.

Several commenters recommended that the definition of "passenger access areas" be clarified in the final rule to state that no person, including employees, workers, and vendors, would need a TWIC to have unescorted access to a passenger access area on a vessel.

We have not amended the language as suggested, but agree with the commenters' concept. The proposed, and now final, definition of "passenger access area" states that these areas are not part of the secure area of the vessel. Thus, anyone requiring unescorted access to the passenger access area ONLY does not need to have a TWIC,

as he or she does not need unescorted access to a secure area. This covers passengers, employees, other workers, and vendors.

(d). Monitoring

One commenter felt that the definition of "monitoring" as used in current regulations and the TWIC NPRM, was ambiguous, confusing, and should be deleted. We disagree. The NPRM did not propose to change the definition of monitoring, and as such we are not making any changes in the final rule. For an explanation of what was meant by that term, *see* the final rule titled "Implementation of National Maritime Security Initiatives," issued on October 22, 2003 (68 FR 60448).

(e). Breach of Security

One trade association recommended that the definition for "breach of security" as used in current regulations and the TWIC NPRM be clarified to allow certain individuals without a TWIC in secure areas, such as escorted persons and foreign seafarers conducting authorized ship's business. The commenter also recommended that the guidance in parts 104 through 106 be amended to clarify this.

Neither the NPRM nor the final rule amend the definition for "breach of security." As stated in the NPRM, "[c]ircumstances that trigger the reporting requirement[s] in § 101.305 are highly fact-specific and difficult to define comprehensively." (71 FR 29417). Generally speaking, finding properly escorted persons within a secure area would not, in and of itself, constitute a breach of security. One situation that would, with certainty, however, is finding someone unescorted within a secure area without a TWIC. This would constitute a breach of security. We will be issuing new guidance for parts 104 through 106, in the form of a NVIC, and will be sure to include provisions on what could constitute breaches of security or suspicious activity in the context of TWIC.

(f). Escorted/Unescorted Access

Several comments requested clarification and additional guidance on the definition of "escorting." Several commenters requested additional clarification about the level of surveillance for personnel without a TWIC, and supported the use of surveillance and monitoring technology instead of physical escorting, or the use of one escort to monitor multiple individuals. The commenters said that constant, one-on-one supervision would be unduly burdensome.

Commenters also stated that the escorting and recordkeeping requirement would be too burdensome in terms of manpower, cost, and recordkeeping. Many of these commenters interpreted the definition to require the physical presence of one escort for each individual without a TWIC at all times while in a restricted area. Some of these commenters provided examples of situations where the requirement would be too burdensome. One port authority stated that it typically has over 100 temporary workers on site that would require escorts. Another commenter was concerned that the rule may prevent shore leave for European Union workers not holding a TWIC, particularly where an escort was unavailable or the regulations were interpreted inconsistently at different ports. One trade association felt that the requirement for escorting would be too burdensome for facilities without the manpower to escort individuals without TWIC, particularly in emergency situations when the workforce has been displaced. One commenter felt that the escort provisions should be unnecessary for foreign maritime facilities complying with the International Ship and Port Facilities Security Code (ISPS Code).

Several commenters were concerned about the need to escort repairmen, maintenance crews, truck drivers, delivery men, crews doing dockside checks of their vessel, musicians, caterers, and other workers, and the need for escorting during weekends and non-business hours when escorts might not be available. One commenter stated that it would have to provide escorts for technical representatives of foreign equipment manufacturers to work on its foreign-built (but U.S.-flagged) vessels. The company also said the rule would be "problematic" because it would require a constant escort for foreign owners of U.S.-flagged vessels who visit the vessels. They also stated the rule might disadvantage U.S. ship management companies that operate U.S.-flagged vessels for foreign owners.

As noted above in the section discussing changes to the Coast Guard provisions, we have amended the definition of escorted access to clarify that when in an area defined as a restricted area in a vessel or facility security plan, escorting will mean a live, side-by-side escort. Whether it must be a one-to-one escort, or whether there can be one escort for multiple persons, will depend on the specifics of each vessel and/or facility. We will provide additional guidance on what these specifics might be in a NVIC. Outside of restricted areas, however, such physical

escorting is not required, so long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual "under escort" be found in an area where he or she has not been authorized to go or is engaging in activities other than those for which escorted access was granted. Again, we will provide additional guidance with more specifics in a NVIC.

Additionally, as discussed above, the reporting and recordkeeping requirements proposed in the NPRM have been removed from this final rule. We will take the comments on these requirements into consideration when we begin a new rulemaking on reader requirements.

One commenter felt that the definitions of "escorting" and "unescorted access" are in conflict, and recommended that the definition of "unescorted access" be broadened to include either an escort or monitoring sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted.

One commenter felt that the definition of escorting was in conflict with the requirement in § 105.290(d) to provide additional security to monitor holding, waiting, or embarkation areas, because passengers that do not hold TWICs may be in those areas. The commenter expressed concern that this conflict could result in inconsistent requirements, with some government officials requiring each passenger to be accompanied one-on-one by security personnel.

"Escorting" means "ensuring that the escorted individual is continuously accompanied while within a secure area in a manner sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted." As stated above, we did not intend for the term escorting to always mean a one-to-one side-by-side escort, and we have added to the definition to clarify that outside of restricted areas, monitoring will meet the definition of escorting. We believe that the requirements in § 105.290(d) are sufficient to meet the definition of "escorting" when passengers are in holding, waiting, or embarkation areas so long as the monitoring provisions of the facility's approved security plan are in place.

One commenter recommended that the definition be clarified to state that the escort must hold a TWIC. This would prevent two individuals without TWICs from escorting each other.

We have included the requirement that all escorts be TWIC-holders in the actual access control provisions of parts

104, 105, and 106. We have added language to the definition to specifically state that individuals without TWICs may not enter restricted areas without being escorted by an individual who holds a TWIC, with certain exceptions for new hires.

One port authority recommended that the escorts be limited to a subset of TWIC holders, as is done in the aviation sector, and that a limit on the number of individuals a single person can escort be established. We have no limits on who can serve as an escort, other than the requirement that all escorts hold a TWIC. Owners/operators are free to establish more stringent requirements for their escorts if they so desire. As stated above, we will be issuing a NVIC that will provide more detail on how many individuals each escort can accompany at one time.

One commenter requested clarification on who was qualified to be an escort and was concerned that they would need to use an outside security service to serve as escorts. It is not our intention to require outside security services in order for an owner/operator to be able to provide escorts. We will provide more guidance on what is expected of escorts in our NVIC, but generally we expect that any escort be able to respond quickly should any of the individuals that he or she is escorting enter (or attempt to enter) an area they are not authorized to be in or engage in activities other than those for which escorted access was granted.

One commenter felt that the definitions of "escorting" and "unescorted access" are in conflict, and recommended that the definition of "Unescorted Access" be broadened to include either an escort or monitoring sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted.

The definition of "unescorted access" in the final rule provides flexibility, allowing owners/operators to designate which individuals need unescorted access, which need to be escorted, and which need to be banned from all access based on their individual circumstances. The Federal government will take appropriate action against known or suspected terrorists or illegal aliens, preventing them from gaining even escorted access to secure areas. However those persons who represent "security threats" due to past criminal activity may not constitute a risk when escorted.

As we noted above, we did not intend for the term escorting to always mean a one-to-one side-by-side escort. In fact, outside of restricted areas, such side-by-

side escorting is not necessary, so long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual "under escort" be found in an area where he or she has not been authorized to go. As stated above, we will provide additional guidance with more specifics in a NVIC.

(g). Recurring Unescorted Access

Many commenters supported the provision allowing the holder of a TWIC who regularly enters and departs a secure area on a vessel on a continual basis to do so without verifying the TWIC for each such event. The commenters felt that screening employees that access secure areas frequently would be burdensome. One commenter stated that this provision is needed by operations with few employees. Some of these commenters supported expanding this provision to include facilities. One commenter recommended that facilities allow recurring unescorted access without TWIC verification, when the validity of an individual's TWIC has been confirmed within the prior thirty days during Maritime Security (MARSEC) Level 1, but that at MARSEC Level 2 TWIC verification be conducted each time the individual accesses the area.

One commenter recommended the definition be revised to "* * * authorization to enter a vessel or facility on a continual basis after an initial personal identity and credential verification, as outlined in the vessel or facility security plan." The commenter stated that this modification will provide significant relief for facilities during MARSEC Level 1.

We reviewed these comments and recognize that recurring unescorted access might be a valuable and sensible tool for both vessels and facilities. However, because the requirements for readers and owner/operator TWIC verification have been removed from the access control provisions of this final rule, the term is no longer used within the access control provisions of subchapter H. Despite this fact, we have retained the definition, and expect that it will be used in a future rulemaking to impose reader requirements. Any NPRM on that issue will include consideration of expanding the concept to any vessel or facility with a small enough contingent of regular employees that allowing such access would not present a significant security risk.

(h). Secure Area

There were numerous comments on the proposed definition of secure area. One commenter requested clarification

on where card readers need to be located for secured and restricted areas. When the NPRM on reader requirements is published, we will include clarification on this subject, where appropriate.

Many commenters felt that the use of the terms "secure area" and "restricted area" was confusing, and that additional clarification or changes to the definitions or use of these terms be made. Several commenters believed that these terms meant the same thing, and recommended using either "secure area" or "restricted area", but not both. Several commenters felt that "secure area" should not be defined as "restricted area" at low consequence facilities. One commenter recommended that any facility be given the flexibility to designate its existing restricted areas as its secure areas in its TWIC Addendum. The commenter recommended that specific provisions in the proposed regulations that could be interpreted as preventing this, such as the requirement that "appropriate personnel know who is on the facility at all times" (33 CFR 105.200(b)(18)) and the record keeping requirements (33 CFR 105.225(b)(9)) should be revised to make it clear that they only apply within the secure areas designated in the TWIC Addendum. One commenter recommended that only the term "secure area" be used, while other commenters recommended that only the term "restricted area" should be used. Many commenters recommended that the definition of "secure area" should be aligned with, or made the same as, the existing definition of "restricted area" used in existing security plans. The commenters felt that this would be more consistent with existing regulations and security plans and would allow flexibility without reducing security. These commenters argued that having different definitions would result in unnecessarily increasing access restrictions in areas that are restricted to employees only but are not essential for security, such as galleys and storage areas. Some commenters recommended that the final rule include a definition of "employee only area" or "owner-controlled area" for such areas, and that TWIC not be required for them.

Two commenters recommended that the term "secure area" be defined more narrowly than "restricted area." One of these commenters was concerned that defining the terms "secure area" and "restricted area" to be the same would be costly for facilities and vessels that have designated in their security plan their entire facilities and vessels as a "restricted area."

Several commenters recommended that if “secure area” and “restricted area” are defined as coextensive, facilities should have flexibility in determining which “secure areas” require TWIC. Another commenter recommended that if “secure area” and “restricted area” be defined as coextensive, the agency create a definition for “security sensitive areas” requiring TWIC that would be a subset of “secure areas.” Multiple commenters requested that if these terms do have different meanings, the final rule should explain the difference, and identify the difference in access restrictions required for them.

One commenter was concerned that the Coast Guard would not accept the “restricted areas” established in existing security plans as “secure areas.” This commenter felt that vessels and facilities should have the flexibility to define existing areas designated as “restricted areas” as “secure areas” to avoid expending resources on areas that are not important to security.

Multiple commenters were concerned that the definitions of “secure area” or “restricted area” would result in inconsistent application by regulators at different facilities. One commenter was concerned that their entire facility has been determined to be a secure area, and thus all of their employees would require a TWIC. Some commenters recommended that small facilities be allowed to define areas as being “secure areas” only when a vessel is present.

Several commenters were concerned that the definition of “secure area” was too broad, and would require TWIC for any area with any access restriction, such as a fence. Commenters were concerned that this would result in their entire vessel or facility being designated as a “secure area.” Many of these commenters felt that they could not meet such a requirement, or that such a requirement would be unnecessary for security. One commenter expressed concern that this might result in numerous Transportation Security Incidents.

One commenter recommended that the first sentence of the proposed rule be rewritten to read, “Secure area means the area on board a vessel or at a facility or outer continental shelf facility which the owner/operator has designated as requiring a transportation worker identification credential (TWIC) for a person obtaining unescorted access, as defined by a Coast Guard approved security plan.”

Multiple commenters recommended that the final rule clarify that facility owners and operators have broad flexibility in designating “secure areas,”

and that the Coast Guard readily approve such designations. These commenters felt that this was necessary to minimize the costs and disruptions from the rule.

One commenter recommended that the proposed rule be amended to include a process for limiting the portions of sites to be covered by the rule based on security vulnerability criteria, which would certainly include barge unloading facilities and possibly other areas designated as “restricted” in the site’s FSP developed under MTSA.

As noted above in the discussion of changes to the Coast Guard provision of this rule, we did not intend for the terms “secure area” and “restricted area” to be read as meaning the same thing.

As also noted above, we recognize that many facilities may have areas within their access control area that are not related to maritime transportation, such as areas devoted to manufacturing or refining operations. The individuals working in these non-maritime transportation areas may rarely, if ever, have a need to access the maritime transportation portions of the facility. As such, we are giving facility owners or operators the option of amending their FSP to redefine their secure area to include only those portions of their facility that are directly related to maritime transportation or are at risk of being involved in a transportation security incident. Redefining the secure area does not necessarily reduce the original facility footprint covered by the FSP where security measures are already in place. That can only be achieved by a reevaluation of the facility as a whole. Instead, the amendment will only effect where TWIC program requirements will be implemented. Additionally, any secure areas must have an access control perimeter which ensures only authorized individuals with valid TWICs have unescorted access. These amendments must be submitted to the cognizant COTP by July 25, 2007.

One commenter expressed a desire for Coast Guard to support allowing a facility owner/operator to modify their FSPs by maintaining a significant level of security for the entire facility, while enhancing security for narrower area of the site. This commenter proposed the following language for the final rule preamble: “Facility owner/operators are encouraged to review, and revise as necessary, their Facility Security Plans to apply TWIC requirements to those portions of the site that (i) trigger MTSA regulation, (ii) can be reasonably separated through access controls from other parts of the facility; and (iii)

require a higher degree of security protection. Coast Guard will review and approve these changes to the FSP so long as the facility demonstrates that (i) it can maintain existing security at the balance of the facility, and (ii) restricted access controls (including TWIC access controls) have been provided for the area that will have heightened security.”

We agree with the substance of this comment. While the exact recommended verbiage has not been incorporated into the final rule, we believe the intent and proposed flexibility has. Facility owners and operators will continue to be responsible for drafting and submitting their unique security plans for Coast Guard approval. As noted above, greater flexibility has been afforded to facility plan submitters, allowing them to redefine their secure area to include only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident.

We realize that there may be some owners and operators of vessels that would like the same option. However, vessels present a unique security threat over facilities in that they may not only be targets in and of themselves, but may also be used as a weapon. Due to this fact, we will continue to define the entire vessel as a “secure area,” making exception only for those special passenger and employee access areas which are discussed below. Vessel owners/operators need not submit an amendment to the VSP in order to implement these special areas, however they may do so, following the procedures described in part 104.

Commenters also requested clarification on whether the term “secure area” is intended to include passenger access areas as defined under 33 CFR 105.106. These commenters recommended that the passenger access areas not be defined as “secure areas.”

“Passenger access areas” are, by their definition, not secure areas. They will, however, exist solely within the secure area of the vessels on which they are implemented. As such, they will operate as “pockets” within the secure area.

One commenter stated that small passenger vessels and facilities where they moor would be at a small risk of a terrorist attack. The commenter recommended that the final rule state that such vessels and facilities do not have any “secure areas.”

We do not agree with this comment. During the MTSA rulemaking process, the Coast Guard evaluated all vessels and facilities to determine which of those are at a high enough risk of a

Transportation Security Incident (TSI) to warrant imposing the security plan requirement. Small passenger vessels and the facilities that they use were determined to pose a high enough risk to warrant imposition of the security plan requirement. We do not believe that circumstances have changed to warrant a change to those requirements. We have, however, provided some relief to small passenger vessels in this rulemaking by allowing them to carve out passenger and employee access areas (explained elsewhere in this final rule), which will help minimize the "secure area" on board.

One commenter was concerned that since secure areas are defined in the owner or operator's threat assessment (which is approved by the Coast Guard, but is not publicly available), a business operating at the port, vessel, or facility for the first time would not know what areas are designated as "secure" and whether they need a maritime TWIC.

The threat assessment approved by the Coast Guard addressed restricted areas, not secure areas. We have defined secure areas as the access control areas of vessels and facilities, which should provide enough guidance to new businesses, as the area over which a vessel or facility exerts access control should be readily visible to anyone approaching that vessel or facility for access.

One commenter also requested clarification on whether "secure areas" corresponds to existing security classification existing under the ISPS Code.

The comment is unclear. The ISPS Code uses the term restricted area, and as discussed above, we do not intend for the secure area to mean the same thing as restricted area. In that regard, this final rule does not correspond with the ISPS Code. However, we note that the definition we have provided will not interfere with a vessel or facility meeting the requirements of the ISPS Code.

One commenter noted that safety issues surrounding needed access to "secure areas" in an emergency are not addressed. Another commenter stated that access to secure areas cannot be restricted in an emergency. We recognize this issue and have added a paragraph to § 101.514 that clarifies emergency personnel need not have TWICs to obtain unescorted access to secure areas during emergencies.

Two commenters recommended that the term "secure area" be revised to read "Secure area is used as defined in 33 CFR 101."

We disagree. The definitions found in 33 CFR part 101 apply to all of

subchapter H, therefore it is not necessary to constantly refer back to part 101 when, in parts 103 through 106, we use a term defined in part 101.

2. General Comments on Applicability

Many commenters had questions and/or concerns for TSA and Coast Guard related to the applicability of the proposed rule. One asked what the TWIC requirements would be for a CDC facility that is in a separate location on port property, since it is not a secure maritime facility and thus does not fall under the security regulations of 33 CFR part 105.

Another commenter posed several questions for TSA and Coast Guard: Will the unlicensed crew members on small passenger vessels certificated for less than 150 passengers under "Subchapter K" need to hold a TWIC? Will unlicensed crew members on passenger vessels carrying more than 12 passengers, including at least one passenger-for-hire, on an international voyage, which can include large charter yachts of up to 500 Gross Register Tonnage (GRT), be required to carry a TWIC? Will deckhands on barges subject to "Subchapters D or O" be required to obtain a TWIC? Will deckhands on towing vessels greater than 26 feet in length be required to obtain a TWIC?

One commenter noted that every terminal under MTSA is unique, which is why they are required to have FSPs and suggested that 33 CFR part 105 be used as a baseline and to allow terminals to write their specific plans to ensure security and ease of commerce thus allowing the terminal operators to determine if individuals without the TWIC may have unescorted access to the terminal. One commenter shared their experience implementing legislation similar to the TWIC via Florida Statute 311.12. The commenter suggested adding a grandfather component to the proposed rule to allow current personnel working in the maritime industry certain considerations. The commenter went on to note that if they had not implemented a grandfather component to Florida Statute 311.12, the smooth operation of commerce would have come to a halt.

Many commenters, including individuals, marine services companies, barge lines, cruise lines, towing companies, and marine maintenance companies, argued that they already had adequate security plans, restrictions, testing procedures, personnel procedures, and other safeguards in place, some of which were approved by the Coast Guard. One local government commenter said that TSA should

exempt any facility from the TWIC requirements that had a FSP already in place. Another commenter noted that in the absence of security incidents at any scrap yards relating to maritime transportation and small port facilities that receive bulk aggregate materials, the FSP should be sufficient for addressing risks at such facilities.

MTSA was clear and unambiguous, leaving little if any room for agency interpretation. Essentially, all individuals must hold a TWIC in order to be eligible for unescorted access to secure areas of MTSA regulated facilities or vessels. In addition, the statute was very clear that all credentialed Merchant Mariners will be issued a biometric identification card, which will be the TWIC. Where needed and allowable under the statute, certain arrangements or exemptions were proposed and modified as the result of the public comments to identify special cases where individuals without a TWIC or who are unable to obtain a TWIC can continue to work aboard MTSA regulated facilities or vessels, subject to additional security provisions.

As a result of the public comments and concern regarding the potential negative impact on industry resulting from the requirements to implement a TWIC system, greater flexibility has been afforded to facility owners/operators by allowing them the option, in revised § 105.115, to redefine their "secure area" as only that portion of their access control area that is directly related to maritime transportation. Other definitions, such as "passenger access area" and "employee access area," will also provide greater flexibility in assisting regulated entities with enhancing security while meeting the new regulations. Additionally, provisions have been included, as discussed more specifically below, to allow limited access to new hires under specific conditions, and to persons who have reported their TWIC as lost, damaged or stolen and are awaiting replacement cards.

One commenter recommended utility fuel-handling facilities be the only facilities subject to the TWIC program. The commenter also recommended that the TWIC be required for such facilities only when the facility is being used for off-loading.

As stated earlier, the MTSA of 2002 clearly and unambiguously ruled out blanket waivers for specific industry segments or specific job descriptions. With very limited exceptions, all individuals must hold a TWIC in order to be eligible for unescorted access to secure areas of MTSA regulated facilities or vessels.

(a). Applicability—Requests for Exemptions

Numerous commenters requested exemptions from the TWIC requirements for the following industries, vessels, and facilities:

- U.S.-flagged passenger vessels;
- U.S.-flagged mobile offshore drilling units (MODUs) and offshore supply vessels (OSVs) operating outside the geographic boundaries of U.S. jurisdiction, employing non-citizen workers;
- Other U.S. flagged vessels employing non-citizen crewmembers under the provisions of 46 U.S.C. 8103(b)(3) or (e);
- Inland tugboat, towboat, and barge industry;
- Small and/or isolated low consequence ports, facilities, or vessels;
- Facilities with security requirements that are equivalent or more stringent than the TWIC (*e.g.*, shipyards that currently meet existing DOD credentialing and security plan requirements);
- Facilities and vessels participating in aggregate stockpile and loadout activities;
- Tall ships operating under the U.S. flag and educational sailing programs for school children;
- Bunkering and gas support facilities; and
- U.S. vessels undergoing repairs at a foreign port or facility.

The commenters presented various arguments to support their requests for exemption. Some commenters noted that exemption criteria should be added to the proposed rule indicating that vessels and facilities that were deemed low risk during a risk assessment should not fall under the TWIC requirement, because TWIC places an unwarranted burden on these vessels and facilities with little added security benefit. For example, one commenter requested that oil and gas support facilities and bunkering facilities be exempted from the TWIC requirements. Another commenter asked for an exemption since their activities and their location are low risk, predominately carrying bulk and break bulk products within the Great Lakes.

Similarly, other commenters argued that small vessels (*e.g.*, inland towing vessels, small passenger vessels) or small ports should be exempt from the TWIC requirements because the workers know each other and unknown visitors are infrequent. These commenters argued that the intent of the TWIC system, to identify those people who pose a threat, would not be served by installing card readers on small vessels

or in small ports. They stated that identifying someone who does not belong is not difficult on these small vessels and in these small ports, and can be accomplished visually. They claimed that the proposed rule would only add cost to these industries with little to no benefit to maritime security. For example, many commenters noted that the crews on inland towing vessels are predominantly U.S. nationals who already comply with the security regulations in 33 CFR parts 104 and 105, so requiring TWICs for this industry would be costly and would result in few improvements in maritime security. In addition, several commenters from the small passenger vessel industry requested that subchapter K and T vessels operating in restricted waters and routes be exempt from the proposed rule.

More specifically, some commenters noted that vessels under a specific tonnage should be exempt from the TWIC requirements. One commenter asked that vessels of less than 500 regulatory tons GRT and 6,000 International Tonnage Convention (ITC) tons be exempt from the requirements. Another commenter asked that vessels less than 100 gross tons with undocumented workers be exempt from the proposed rule.

Many commenters argued that U.S.-flagged MODUs and offshore supply vessels (OSVs) operating outside the geographic boundaries of U.S. jurisdiction, employing non-citizen workers should not be required to obtain a TWIC. One commenter argued that in some countries the law requires these vessels operating on the continental shelf to hire local crewmembers, so requiring escorts for all of these crewmembers would place a large burden on these vessels and cause them to be unable to work overseas. In addition, the commenters argued that there is little threat posed by these vessels that are located thousands of miles from the U.S. coast. More than one commenter stated that the ISPS Code and its implementing regulations in SOLAS recognize the need for MODUs and OSVs to employ non-U.S. citizens in their crew and apply shelf-State standards instead of flag-state standards. The TWIC program should recognize the need for these vessels to employ non-U.S. citizens as well.

One commenter stated that it is their understanding that foreign-flagged MODUs (OCS facilities) that are on location on the OCS would be excluded from the requirements, since foreign vessels with valid ISPS Code certificates are in compliance with 33 CFR part 104 (except 104.240, 104.255, 104.292, and

104.295) and all foreign vessels are exempt from TWIC requirements under 33 CFR 104.105(d). The commenter asked for confirmation that this understanding of the proposed rule is correct. In addition, they requested confirmation that a MODU that is not regulated under part 104, and therefore not required to implement TWIC provisions, but is working next to or over an OCS facility that is regulated by part 106, and therefore is required to implement TWIC provisions, would be exempt from the TWIC requirements.

In addition to requests for exemptions for industries, vessels, and facilities, many commenters requested exemptions for the following types of workers:

- Employees who work at small ports, facilities, or vessels;
- Merchant seamen who are U.S. citizens and hold current U.S. Coast Guard licenses, Merchant Mariner Documents (MMD), certificates of registry, and STCW documents;
- Employees on vessels under 100 gross tons;
- Contract security guards who have already undergone a DOJ background investigation;
- Crewmembers, service technicians, or repair persons performing vessel maintenance and repairs;
- Hotel staff and passenger vessel staff;
- Seasonal or short term workers which access needs of less than 90 days;
- Cadets from U.S. maritime academies;
- Emergency response personnel;
- 15.702(b) crew and other authorized foreign nationals boarding U.S. vessels overseas;
- Employees who must continuously enter and exit secure areas (*e.g.*, baggage handlers at a cruise ship terminal);
- Port chaplains or other religious personnel;
- Workers who are not involved in the transportation industry; and
- Vessel agents.

The reasons presented by the commenters for granting the workers' an exemption were varied. Some commenters argued that passenger vessel staff who work within the same areas as the passengers who are not subject to the requirement should not be required to obtain a TWIC.

Commenters argued that crewmembers, service technicians, or repair persons performing vessel maintenance and repairs should not be required to obtain a TWIC because they do not present a security risk and additionally because there are not enough vessel and facility staff to escort these workers.

One commenter asked that the proposed provision exempting foreign vessels be expanded to also exempt "foreign nationals employed on U.S. vessels under the provisions of 46 CFR 15.720(b) or who are authorized visitors aboard a U.S.-flagged vessel operating from or in foreign ports."

Many commenters requested exemptions for emergency response personnel and law enforcement officers.

More generally, commenters suggested that workers should be exempt from the TWIC requirements until they go to work for a company that needs to conduct business in a secure area. In addition, commenters requested that workers without access to restricted areas of vessels or terminals not be required to obtain a TWIC.

MTSA was clear and unambiguous and ruled out blanket waivers for the requested industry segments or specific job descriptions. Essentially, all individuals must hold a TWIC in order to be eligible for unescorted access to secure areas of MTSA-regulated facilities or vessels. Where needed and allowed by statute, certain arrangements or exemptions were proposed and modified as the result of the public comments to identify special cases where individuals without a TWIC or who are unable to obtain a TWIC can continue to work aboard MTSA-regulated facilities or vessels subject to additional security provisions.

These special cases include the foreign vessel exemption, a new provision within the definition of secure area stating that in certain circumstances, U.S. vessels operating in foreign waters do not have secure areas, the passenger and employee access areas, and the provision allowing part 105 facilities to amend their security plans to limit their secure area to only those portions of their facility that are related to maritime transportation.

When issuing the regulations found in 33 CFR chapter I, subchapter H (known as the Coast Guard MTSA regulations), which establish who must submit a security plan, the Coast Guard utilized a risk based approach to identify and separate those particular facilities and vessels which pose a higher risk from those which pose a lower risk. While we agree with the argument that one MTSA-regulated facility or vessel can pose a lower risk than another MTSA regulated facility or vessel, the fact remains that all have already been determined to present a high enough risk of a TSI to warrant their inclusion in the MTSA regulations. The statute requires all MTSA regulated vessels and facilities to comply with the access control requirements by requiring

TWICs for unescorted access to secure areas.

As a result of numerous comments and concerns regarding reader usage and installation aboard facilities and vessels in addition to emerging technology, this final rule addresses use of the TWIC as a visual identity badge and does not require use of readers. We will consider those comments requesting that the risk among all MTSA regulated vessels and facilities be reevaluated when we propose reader standards in a subsequent rulemaking.

Understanding the unique situations where successful commerce and support of the maritime industry is dependent upon legal employment or boarding of foreign mariners or crew while operating outside of U.S. waters, we determined that we must change some language from the proposed rule. As such, we are adding a provision to the definition of secure area in § 101.105 that states that U.S. vessels operating under the waiver provisions found in 46 U.S.C. 8103 (b)(3)(A) or (B) have no secure areas. These waiver provisions allow U.S. vessels to employ foreigners as crew in certain circumstances. As soon as the vessel ceases operating under these waiver provisions, it will be deemed to have secure areas as otherwise defined, and TWIC provisions will apply.

Additionally, facility owners/operators can affect the population of those who will need to obtain a TWIC by taking advantage of the option given to them in revised § 105.115 and redefining their "secure area" as only that portion of their access control area that is directly related to maritime transportation. The Coast Guard must approve such modifications.

(b). Applicability—Foreign Vessels

One commenter supported the proposed exemption for foreign flag vessels calling on U.S. ports. The commenter stated that this would include not requiring a valid TWIC to access vessel-designated restricted areas and the need for TWIC readers aboard foreign flag vessels. However, many commenters disagreed with this provision for various reasons. Some commenters stated that there is a need for application of international standards to all ships, U.S. and foreign, to maintain a level playing field and prevent economic discrimination against U.S. ships. For example, one commenter stated that security within the Gulf of Mexico will not be ensured until the foreign vessels that routinely operate in support of the offshore oil and gas industry, and call on Gulf ports such as Fourchon, Galveston, Mobile,

etc., are held to and comply with equivalent standards.

Another commenter urged that an accurate cost-benefit analysis must factor in the cost of vessel operating companies that are forced out of business because they cannot compete with foreign competitors in the Gulf of Mexico who have been exempted from these requirements.

Other commenters argued that the proposed regulations overlook the area of greatest interest to national security, namely the traffic of foreign vessels and foreign seafarers at U.S. ports and maritime facilities, while imposing additional regulation on American mariners who already undergo thorough vetting, and U.S. vessels that already operate under a vessel security plan compliant with the MTSA. One commenter claimed that a security threat posed by individuals on a foreign-flagged vessel moored at a U.S. port is no less of a security threat than persons aboard a U.S. vessel, and objected that TSA has decided to forgo security requirements for foreign-flagged vessels. One commenter expressed that DHS has not conducted any analysis as to whether foreign mariners who do not participate in SOLAS or ISPS pose homeland security threats. One commenter stated that the Coast Guard has not fully considered the impact of its requirement to grant access to foreign nationals who have not been vetted by TSA.

One comment stated that because foreign mariners are not required to hold a TWIC under the proposed rule, if the entire terminal is classified as a "secure area," crewmen that have docked at berth and have been cleared by CBP must be escorted every time they leave the "restricted area" of the pier. The commenter notes that if they are already in the restricted area they do not have to be escorted, but if they enter that part of the secure area that is not restricted, they must have an escort. The commenter asked that, since CBP has already made a determination whether these mariners pose a risk to our country, why then does a low consequence terminal have to make sure they are escorted if they pose no risk?

One comment said the proposed rule does not clearly indicate whether a foreign vessel must obtain, deploy, and operate TWIC readers at its access points on the vessel. However, the commenter said that the proposed rule appears to exempt foreign vessels from using TWIC readers.

Foreign vessels carrying valid ISPS Certificates do not fall within the TWIC applicability of the MTSA, as they are not carrying security plans approved by

the Secretary under 33 U.S.C. 70103. MTSA requires compliance with TWIC requirements for vessels or facilities whose plans include an area designated as a secure area by the Secretary for purposes of a security plan approved under sec. 70103. The vast majority of foreign vessels do not submit their plans to the Secretary, and therefore are not "secure areas" even when the foreign vessel is docked at a U.S. port. However, when docked at a U.S. port, individuals on the foreign vessels are subject to the facility's security plan—including TWIC and escorted access requirements—if they wish to leave the foreign vessel.

We do not agree that sec. 102 of the MTSA applies to foreign seafarers arriving on foreign vessels. The TWIC process cannot practically or meaningfully be applied to foreign mariners, who would not likely have the means to get to enrollment centers or to return to claim and activate their credentials, nor would any be able to present the appropriate identity documents, or meet the requirement for lawful presence. Requiring foreign seafarers to present a TWIC would mean that before being allowed off of a foreign vessel, each foreign seafarer would need to come to the United States to enroll in the TWIC program, and then again to pick up their TWIC. It is also not clear that such a provision would provide any security benefit, as the criminal background checks that are done as part of the TWIC security threat assessment would have very little meaning, since it is unlikely that a foreign seafarer will have a criminal record in the United States, and the additional background checks are done during the visa application and CBP screening processes (see below). Finally, placing such requirements on foreign seafarers would certainly affect the treatment U.S. mariners receive in other countries.

We also disagree that the TWIC subjects U.S. maritime workers and mariners to stricter processes than foreign seafarers. Currently, foreign seafarers arriving on foreign vessels are required to have a U.S. visa, issued by the Department of State subsequent to at least one face-to-face interview and a vetting process that is similar to TWIC vetting. Upon arrival in the U.S., foreign mariners are not allowed to leave the vessel until and unless they are allowed entry after inspection by a CBP Officer. Those seafarers that arrive without a visa or a CBP issued waiver are restricted to the vessel. Seafarers that are allowed to leave the vessel are subject to the security provisions of the facilities where their vessel is moored, including the conditions by which they are allowed to traverse the facility, and

will be required to have escorted access through secure areas of the facility.

One commenter urged that a further provision be added at new § 104.105(e) to read as follows: "(e) Foreign nationals employed on U.S. vessels in accordance with the provisions of 46 CFR 15.720 or who are authorized visitors aboard U.S. flag vessels operating from or in foreign ports are not subject to the TWIC requirements found in this part."

As noted above, we are adding a provision to the definition of secure area in § 101.105 that states that U.S. vessels operating under the waiver provisions found in 46 U.S.C. 8103 (b)(3)(A) or (B) have no secure areas. These waiver provisions allow U.S. vessels to employ foreigners as crew in certain circumstances. The effect of this change is to exempt these vessels from the TWIC requirement while they are operating under the referenced waivers. As soon as the vessel ceases operating under these waiver provisions, it will be deemed to have secure areas as otherwise defined, and TWIC provisions will apply.

Many commenters stated that not requiring foreign vessels and foreign crews to obtain a TWIC would be detrimental to U.S. maritime security. One commenter noted that this policy would put U.S. offshore oil and gas supplies at risk. One commenter pointed out that currently a large portion of the ships transporting oil and hazardous materials are foreign vessels with foreign crews.

Another commenter noted that 95 percent of the vessels sailing from international waters into U.S. ports are crewed by foreign mariners, so although vetting these foreign mariners would be very difficult it is necessary to enhance U.S. port security. The commenter pointed out that U.S. mariners are already subject to background checks during the licensing procedure, so including U.S. mariners, while exempting foreign mariners from the TWIC program will not enhance U.S. port security.

Numerous commenters expressed concern about uncredentialed foreign mariners. One argued that if licensed and documented American mariners must hold a TWIC, foreign workers on American flag vessels should also be required to hold proper security credentials. Many commenters argued the necessity of covering foreign nationals working as drivers in domestic facilities such as ports and foreign crewmen on foreign vessels, such as Liquefied Natural Gas (LNG) tankers. Comments came from a wide variety of maritime and trucking industry associations, and individuals.

Some commenters also stated that ensuring the security of freight moving in from foreign ports was a more important issue than TWIC.

One commenter noted that under the proposed rule many commercial fishing vessels will not be required to obtain a TWIC. The commenter argued that the TWIC program should include all commercial vessels, since commercial fishing vessels could easily be used as a terrorist target.

We do not agree with these comments. As discussed above, the vast majority of foreign vessels are not required to have a security plan under MTSA and thus do not constitute secure areas for purpose of the TWIC program. In regard to the security concerns cited by the commenters, however, individuals from foreign vessels who wish to leave the vessel while docked at a U.S. port are required to be escorted through secure areas on MTSA-regulated facilities. Further, each and every foreign mariner wishing to step off of a vessel onto U.S. soil must be issued a visa from the Department of State, and be admitted by CBP into the United States.

In addition, the Federal government has a variety of programs in place to identify potential security risks from foreign vessels and crew members entering U.S. ports. For example, the Coast Guard's Notice of Arrival requirements (33 CFR part 160, subpart C), U.S. Coast Guard Port State Control Examinations, vessel escorts, and crew list, cargo and last port of call screening, foreign port inspections and similar programs have been in place for several years to reduce the risk posed by certain foreign-flagged vessels transiting or calling U.S. ports.

Additionally, under CBP's Advance Passenger Information System (APIS) (19 CFR 4.7), vessels (both foreign and U.S.-flagged), must provide manifest information on all passengers and crew no later than 24 hours and up to 96 hours prior to the vessel's entry at a U.S. port. The data that must be provided by the vessel to CBP includes: the country that issued the passport or alien registration number; the passenger's or crew member's full name, date of birth, passport or alien registration number, country of residence, visa number, originating foreign port and final port of destination. *Id.* The manifest information is compared against terrorist watchlist information by CBP.

Commercial fishing vessels are not subject to 33 CFR subchapter H and therefore are not included in the congressional mandate for TWIC. As noted in the interim final rule published on July 1, 2003, titled "Implementation

of National Maritime Security Initiatives,” commercial fishing vessels were determined to be at a low risk of a TSI during the initial risk assessment and therefore were not included in the applicability for 33 CFR subchapter H (see 68 FR 39246–7).

One commenter stated that there are many reasons for foreign seafarers to be allowed to traverse the facility (*i.e.*, reading draft marks, completing a Declaration of Security (DoS), required training, making phone calls, medical and humanitarian needs). The commenter argued that to only mention crew changes and shore leave does not advise facility operators and Federal officials that there are other legitimate reasons for seafarers to be granted access to portions of a facility.

We agree that there are legitimate reasons for foreign seafarers to require limited access to facilities. Recognizing, in particular, that seafarers, whether foreign or U.S., will require access to facility areas to conduct vessel operations, such as reading drafts, adjusting mooring lines, securing shore ties, completing a declaration of security (DoS), and loading stores, we have included a provision to allow mariners limited access immediately adjacent to their vessels to conduct these operations. Limiting the access in this manner takes operational realities into account without adversely impacting security. Also recognizing this need applies to U.S. vessels not covered by 33 CFR part 104 when moored at a part 105-regulated facility, this provision is also granted to U.S. mariners on vessels not covered by part 104 who would not otherwise be required to possess a TWIC.

(c). Applicability—Mariners

One commenter requested clarification about whether every uncredentialed mariner (*e.g.*, crewmember) requiring unescorted access to secure areas of vessels and facilities will require a TWIC. Many crewmembers who have unescorted access to secure areas of vessels and facilities are not required to have credentials (*e.g.*, up to 17,000 crewmembers on inland and river towing vessels up to 1,600 GRT; crewmembers on small passenger vessels up to 100 GRT; and offshore towing vessels up to 100 GRT), noted one commenter. Therefore, the commenter argued that the proposed rule needs to make it clear that every uncredentialed mariner requiring unescorted access to secure areas of the vessels (especially small passenger vessels, offshore supply vessels or facilities) will need a TWIC.

Under this rule, every mariner, whether holding a credential from the Coast Guard or not, who requires unescorted access to a secure area of a MTSA-regulated vessel or facility will need to have a TWIC.

Another commenter, an owner of vessels and facilities, noted that they currently are not required to have VSPs or FSPs, however, the proposed rule indicates that their licensed employees will now need to obtain a TWIC. The commenter stated that making a licensed employee obtain a TWIC when the workplace is non-secure does not make sense. In addition, the commenter noted that only requiring licensed crewmembers to obtain a TWIC, but exempting unlicensed crewmembers, does not make sense. One commenter suggested that this could become very burdensome for the vessels and facilities, since individuals may choose not to obtain a TWIC and thus will have to be escorted while in secure areas. The commenter recommended that TSA and Coast Guard make the TWIC mandatory.

Many individual commenters and commenters from mariners' associations argued that domestic merchant seamen are already required to obtain documentation, and that an additional burden should not be placed on them. Several said that domestic professional mariners should be considered partners in security, because they have a vested interest in a secure workplace. Commenters stressed that the rule should recognize the difference between “bluewater” international operations and “brownwater” domestic operations on inland waterways, because the latter do not pose the same threat to national security. Several commenters also argued that the economic effect of the proposed rule would be to place domestic maritime workers, such as those in the offshore oil and gas industry, at a disadvantage vis-à-vis foreign competitors.

The final rule applies to all licensed mariners, regardless of where they work, and workers needing unescorted access to secure areas of vessels, facilities, and OCS facilities currently regulated by parts 104, 105, and 106. Licensed mariners, regardless of their employer or working location, must obtain TWICs due to sec. 102 of MTSA (46 U.S.C. 70105(b)(2)(B)), which states that the TWIC requirement applies to “an individual issued a license, certificate of registry, or merchant mariners document under part E of subtitle II of this title.” Additionally, the statute requires that any individual requiring unescorted access to secure areas of a vessel or facility regulated by 33 CFR part 104, 105, or 106 obtain a TWIC,

regardless of whether they are licensed or unlicensed. (See 46 U.S.C. 70105(b)(2)(A)). We disagree with the commenters who felt that the TWIC requirement was “not mandatory.” Mariners will not be able to renew their credentials without a TWIC, and vessel and facility owners/operators have an enforceable responsibility to ensure that only persons holding TWICs be granted unescorted access to secure areas. If an individual shows up for work without a TWIC, and his or her employment would call for unescorted access within a secure area, it is the duty of the owner/operator to either turn that individual away or provide an escort, but there is nothing stating that the owner/operator must allow the individual access of any kind. We have provided for limited exceptions to this, to cover newly-hired individuals who have applied for their TWIC but have not yet received it, and to cover those individuals who have reported their card as lost, damaged, or stolen. These provisions can be found in the access control sections of parts 104, 105, and 106.

(d). TWIC Eligibility—Foreign Workers

Many commenters argued that foreign workers who have already obtained work visas and have been cleared by CBP should be allowed to obtain a TWIC, even though they are not resident aliens. For example, some commenters pointed out that trained foreign experts with work visas are often used on U.S.-flagged industrial vessels to assist with specialized work. The commenters argued that requiring an escort for these workers who have already been cleared by the CBP and obtained the appropriate work visas, would be burdensome and unnecessary. These commenters pointed out that just as the NPRM states that Mexican and Canadian truckers need to have access to facilities, offshore vessels need to allow specialized foreign workers on their vessels. Other commenters stated that the proposed rule is more stringent than what is required by law.

Several commenters noted that as a multinational corporation they have foreign employees and foreign business partners at their U.S. facilities, so if these employees and business partners cannot obtain a TWIC it will create a large burden for their corporations. The multinational corporations will face a burden not only from having to provide escorts for their foreign employees and foreign business partners, but also from lost business due to foreign business partners choosing not to work with U.S. multinational corporations due to the extra hassles.

We recognize that this population of workers is essential to the maritime transportation industry and that there would be significant impacts to facilities if they were not able to obtain unescorted access to carry out their work. As a result, we have amended the final rule to allow additional foreigners, holding certain work visas, to apply for a TWIC. These provisions are discussed in more detail in the TSA section below.

We do not believe, however, that TWICs should be issued to anyone who has been granted a work visa and cleared by CBP. While foreign workers—either immigrant or nonimmigrant—may be subject to certain screening to obtain a visa or to enter the country. However, these individuals do not undergo the comprehensive security threat assessment necessary to allow a person unescorted access to a secure facility.

(e). Applicability—Area Maritime Security (AMS) Committee Members

The NPRM proposed requiring that all AMS Committee members obtain a TWIC. Several commenters stated that they agreed with this provision of the proposed rule. For example, one commenter noted that if the rule is not applied equally to all parties it will have little value. Other commenters stated that they did not agree with this provision and felt that AMS Committee members should not have to obtain a TWIC. Some of these commenters argued that the TWIC is not a tool to clear individuals for access to SSI²¹, but is a tool to assist facility and vessel owners in implementing access control. The commenters argued that since some of the AMS Committee members do not need access to secure maritime areas and all of the AMS Committee members have already undergone the screening for access to SSI, the AMS Committee members should not have to obtain a TWIC. In addition, commenters noted that requiring the AMS Committee members to obtain a TWIC would increase the costs associated with membership and thus discourage membership.

After reviewing these comments, we have decided to refine the TWIC requirement in regard to AMS Committee members, as explained above in the discussion of changes to

the Coast Guard provisions of the final rule. The final rule allows individuals to serve on an AMS Committee after the completion of a name-based terrorist check from TSA. FMSCs (*i.e.* COTPs) will forward the names of these individuals to TSA or Coast Guard Headquarters for clearance prior to sharing SSI with these members.

(f). Applicability—Owners/Operators

The proposed rule requested comment on whether owners/operators of vessels, facilities, and OCS facilities should be required to obtain a TWIC, based on their access to SSI. Some commenters argued that requiring those who have already been screened for their access to SSI to obtain a TWIC based solely on their access to SSI would be an unnecessary waste of money and resources. These commenters noted that not all SSI is sensitive enough to require the kind of background check that will be a part of TWIC. A few commenters noted that the owner/operator should determine who in their corporation needs to obtain a TWIC and who needs access to SSI. One commenter noted that this question pertains to 49 CFR part 1520, which was not defined as being within the scope of this rulemaking, although it defines SSI and provides standards for access to and control of SSI. Therefore, although 46 U.S.C. 70105(b)(2)(E) permits the Secretary to determine that individuals with access to SSI must have a TWIC, this issue should be the subject of a separate rulemaking addressing the provisions of 49 CFR part 1520. One commenter argued that owners and operators should be subject to the TWIC requirements, since they have access to SSI. Another commenter argued that owners and operators should be required to obtain a TWIC. They argued that owners' and operators' open access to secure areas and SSI by virtue of their position, warrants their need for the TWIC. This commenter went on to argue that not requiring owners and operators to obtain the TWIC would amount to rank discrimination. They cited the Dubai Ports World controversy as further evidence of the need for owners/operators to obtain a TWIC.

The final rule does not include a requirement that all owners/operators obtain a TWIC. We reviewed all of the comments received and agree with the idea that an owner/operator, due to access to SSI access and ability to control the company, should probably go through a background check. However, our difficulty comes in determining who exactly the owner/operator to be checked is. For small or closely-held companies, this is an easy

answer, and we expect that in the majority of these cases, the owner/operator will get a TWIC due to his/her need to have unescorted access to the vessel or facility. However, larger, multi-national, publicly traded companies pose a much bigger problem. It would be impractical for TSA to run background checks and issue TWICs to anyone holding stock in a company that may own a facility or vessel regulated under MTSA. Additionally, these companies may be structured in such a manner that a bank or several large holding companies are actually the owners, but they have little to no input on the day to day operations at the facility or vessel. We reiterate, however, that any individual, including owners and operators, who wishes to have unescorted access to secure areas must have a TWIC.

As such, we have not included the TWIC requirement for owners/operators in this rule. We will, however, continue to examine the issue, and may propose adding this requirement in the future.

(g). Applicability—Federal/State/Local Officials

The proposed rule states that Federal officials are not required to obtain a TWIC, but must have an HSPD-12 compliant identification. Several commenters agreed with this provision because to obtain the HSPD-12 compliant identification cards, the applicant is subject to the same or more rigorous level of threat assessment that will be required for the TWIC (*e.g.*, background investigations, fingerprints). Other commenters noted technological issues that will need to be resolved if Federal officials are allowed to use HSPD-12 compliant credentials in place of the TWIC. Several commenters emphasized that it is necessary for the TWIC equipment to be able to read the HSPD-12 compliant credentials or validate the cards' continued validity. Another commenter requested that § 101.514(b) be clarified, so it is clear that Federal officials are still subject to the facility's access control requirements and presenting their credentials does not grant them unescorted access to the facility. In addition, several commenters noted that the proposed rule must include a requirement that Federal officials obtain an HSPD-12 compliant ID on the same schedule as the merchant mariners will be required to obtain TWICs and MMCs.

The final rule will require Federal, State and local officials, in the course of their official duties, to present their current agency credentials for visual inspection to gain unescorted access to secure areas. We recognize the

²¹ "SSI" is unclassified information that is subject to disclosure limitations under statute and TSA regulations. See 49 U.S.C. 114(s); 49 CFR part 1520. Under 49 U.S.C. 114(s), the Assistant Secretary of TSA may designate categories of information as SSI if release of the information would be detrimental to the security of transportation. SSI may only be disclosed to persons with a need to know, such as those required to carry out regulatory security duties.

technological difficulties presently facing the evolution of the biometric readers. However, in the future, we anticipate a separate rulemaking to require an HSPD-12 compliant credential to be read by a biometric reader for gaining unescorted access. We must stress that Federal, State and local officials will only use their authority to gain unescorted access in the course of their official duties. Such officials must abide by a facility's or vessel's access control requirements unless extenuating circumstances require otherwise.

Under the proposed rule, compliance would be voluntary for State and local officials because the majority of these individuals undergo a security threat assessment prior to beginning their job. However, several commenters argued that this could be detrimental to maritime security and is problematic for several reasons. First, not all State and local officials undergo a security threat assessment. Second, it would be hard for crew members to determine if the State or local official's credential meets TWIC standards. Third, under this provision State and local officials would not be subject to the background check every five years like other holders of the TWIC. Another commenter noted that there have been instances in the past where local and State agencies have conducted their background checks independently of their employee application process. In addition, another commenter noted that the threat of terrorists posing as armed local or State enforcement officers is great, so there needs to be a more thorough evaluation of these individuals' identity then just showing their ID. Several commenters noted that those with the main responsibility for port security (*e.g.*, port authority police who fall under the State and local system) should be required to get a TWIC, rather than make it optional. One commenter specified that all armed law enforcement officials should be required to obtain a TWIC.

One commenter noted that under § 101.514(c) State and local law enforcement officials would not have to possess a TWIC to gain unescorted access to secure areas. At the same time, § 105.210 would require facility personnel responsible for security duties to maintain a valid TWIC. The commenter said that some ports have a police force comprised of certified police officers who are required to obtain the exact training as State and local law enforcement personnel. The commenter recommended that either § 101.514(c) or § 105.210 be rewritten to recognize these port police and remove the requirement for them to obtain a TWIC.

Federal agencies are already required to implement HSPD-12, therefore there is no need for either the Coast Guard or TSA to do more than require that those credentials be used. We believe State and local agencies may issue similar cards as the Federal government completes implementing HSPD-12. Therefore, we are not requiring State and local officials to obtain TWICs at this time. We may revisit this decision in the future. While all State and local officials may not be required to undergo a security threat assessment comparable to the TWIC, they will continue to utilize their existing authority to board regulated vessels and enter regulated facilities as needed for official business and should continue to be afforded access in accordance with existing approved security plans. However, we encourage local and State officials to obtain TWICs to facilitate access to facilities and vessels when such access is a regular part of their duties.

Regarding the status of "port police" who receive the same training and certification as local or State law enforcement officers being exempt from the requirement to obtain a TWIC, we disagree with the commenter. These individuals can be exempt only if they are actual State or local officials due to their employment status and statutory law enforcement authority.

Other commenters requested clarification of the applicability of the requirements of this final rule to emergency first responders other than law enforcement, such as firefighters and emergency paramedics. We recognize that emergency responders are an important part of any port. We have extended the option to obtain a TWIC to them, but the final rule has also been changed to state that emergency responders will not be required to show a TWIC to gain unescorted access to secure areas during emergency situations, such as natural disasters or transportation security incidents. We do recommend that they obtain a TWIC if they require unescorted access during non-emergency situations.

(h). Applicability—Voluntary compliance

Two commenters wanted § 101.514(d) clarified regarding voluntary implementation of a TWIC program. They stated that the definition of a TWIC program is confusing, and asked "[c]an a voluntary TWIC program be used for badging purposes only, but the vessel or facility owner must still obtain approval of a security plan in order to use the card?" One commenter wants the agencies to explain the opt-in reference from the NPRM, asking why

anyone would opt-in when it carries a mandatory follow-up.

One commenter wants the Coast Guard to insert language into the rule regarding voluntary application of the security plan as opposed to voluntary application of the TWIC program.

As noted above in the discussion to changes to the Coast Guard provisions, this final rule no longer contains provisions allowing for voluntary TWIC programs, therefore it is not necessary to respond to these comments at this time. These provisions have been eliminated due to the fact that neither TSA nor the Coast Guard can, at this time, envision being in a position to approve voluntary compliance before the full TWIC program (*i.e.*, reader requirements) is in place. We will keep it in mind, however, as we develop our NPRM to re-propose reader requirements.

3. Coast Guard Roles

Several commenters expressed concern that the challenge to operators who service multiple ports increases as each COTP is given broad authority to establish and enforce different standards.

We agree that consistency among different COTP zones is important and that different COTP interpretations of a final rule, such as TWIC, can create a challenge especially for those operators who service multiple ports. We also agree that some degree of discretion and flexibility is critical to the successful implementation and enforcement of all Coast Guard regulations throughout a COTP Area of Responsibility. To enhance nationwide consistency of the TWIC regulations, the Coast Guard will continue to create and distribute robust field guidance for use by all COTPs. In most cases, Coast Guard field guidance is available to the public and industry for their own use in preparing for inspections and examinations. Should an operator feel that different interpretations of a particular regulation by two or more COTP are negatively impacting their operation, they are welcomed and encouraged to contact the appropriate Coast Guard District Commander for resolution.

A commenter asked who would enforce the escort requirement and the other TWIC requirements. The Coast Guard will continue to be the primary enforcement authority for all MTSA regulations.

One commenter expressed concern that the Coast Guard has been unable to ascertain and report on the number and types of valid merchant mariner licenses or merchant mariner documents in existence at any time, and that this suggests a limitation in its ability to call

on merchant mariners in response to a national emergency. This comment is addressing the Coast Guard Merchant Mariner Credential (MMC) rulemaking, and so we have not addressed it there.

One commenter requested that the Coast Guard articulate its intentions with regard to production of an identification document complying with the International Labour Organization (ILO) standards for U.S. seafarers.

As the United States is not signatory to the International Labour Organization Seafarers' Identity Document Convention (Revised), 2003 (ILO-185), no plans have been made at this time to produce an identification document complying with that particular standard.

Several commenters suggested that the background checks for TWIC be combined with those required for MMC. Two commenters suggested that TSA perform the security threat assessments for Merchant Mariner Documents (MMDs) as well as TWICs and that the Coast Guard use the results of such assessments in its processing of MMD applications. Others suggested that the consolidated review process should be carried out by Coast Guard.

At this time, the option of having TSA or Coast Guard conduct all the required background checks for individuals who require both the MMCs and the TWIC is not feasible. TSA has established a system and process for ensuring individuals applying for the TWIC undergo a consistent security threat assessment and the Coast Guard already has the authority and process in place for conducting the required safety and suitability checks for mariners prior to issuance of credentials. To create a unique system of background checks for approximately one fifth of the expected initial TWIC population would create the need for additional infrastructure within one agency and raise costs for the government and the entire TWIC population. In addition, the Coast Guard has more expertise and authority over the merchant marine than TSA and is in a much better position to determine whether an applicant is safe and suitable to serve in the merchant marine at the rate or rating sought. At this time, the most efficient and cost effective method available for issuing TWICs to credentialed mariners is to have TSA conduct the security threat assessment and issue the identity document (TWIC) while the Coast Guard continues to issue the mariner's qualification document (MMD/License/MMC).

In addition, requiring only one criminal record review for both security and safety-related crimes by one agency would negatively impact mariner flexibility. If only one background check

were to occur, mariners would be required to apply for their MMC only at the time they applied for their TWIC. As currently proposed, the MMC and TWIC expiration dates need not align. This allows an individual who works at a port to decide later that he or she wants to become a merchant mariner. In addition, for those mariners who already hold a MMD, License or Certificate of Registry (COR), they need not renew their credential upon the initial issuance of their TWIC, because the effective period of their current credential is not affected by this proposed regulation. If we were to require only one background check by TSA for all mariners, the mariner credential would have to come into line with the expiration date of the TWIC. Requiring mariners who already hold credentials to renew so that their credential's expiration date matches their TWIC expiration date is currently impossible from a legal standpoint due to the statutory requirement that Licenses and MMDs must have a 5 year validity period under 46 U.S.C. 7106 and 46 U.S.C. 7302. Such a requirement would inherently shorten that 5 year duration. Finally, requiring only one security/safety/suitability criminal record review by TSA at the time of application would affect individuals who would like to seek raises in grade or new endorsements on their MMC during the 5 year validity period.

One commenter expressed concern about unanticipated impediments to international transportation resulting from TWIC, particularly regarding rail transportation. This commenter urged Coast Guard and TSA to be prepared to respond quickly to interpret the new regulations and address other unanticipated issues.

We agree that both TSA and Coast Guard should be prepared to make modifications to the TWIC program if needed; any amendments will follow existing requirements for changes to published regulations.

One commenter expressed a desire for standardization of the application process for TWIC or MMD across all regions of the country.

We agree that a standard application process for TWIC and MMD (to be replaced by the MMC) is desirable and a reasonable goal. It is our expectation that all forms, instructions and data collection and processing procedures will be standardized, but not combined, for the TWIC and MMC. As stated earlier, some degree of flexibility will be necessary for local TSA and Coast Guard authorities to best serve the local operators and customers. For example, TWIC enrollment center locations,

hours and days of operation are planned to incorporate local industry input.

4. Owner/Operator Requirements

The proposed rule would have required owners/operators of vessels, facilities, and OCS facilities to ensure that security systems and equipment were installed and maintained, including at least one TWIC reader that would meet the standard incorporated by TSA in 49 CFR 1572.23. The proposed rule would have also required that owners and operators ensure that computer and access control systems and hardware are secure.

Several commenters argued that MTSA only mandates TWICs themselves and does not require TWIC readers and their associated equipment. Other commenters were confused as to whether the proposed rule would allow one TWIC reader for an entire vessel and facility or would require a TWIC reader at all access points to secure areas.

Many commenters said that the requirement to place at least one TWIC reader on every vessel would be costly and would not improve security, particularly on small vessels such as towboats. Some commenters argued that their vessel crews are small and that the presence of any unauthorized individuals would be readily apparent. Several of these commenters requested that the final rule waive the requirement for TWIC readers for passenger vessels.

One commenter stated that TWIC readers should not be required in a ship's interior unless required by the vessel's security plan, because existing vessel security plans already adequately address such security concerns. The commenter argued that the locations of TWIC readers should be dictated by the risk assessment performed for the vessel's security plan.

One commenter requested that the final rule allow one TWIC reader for a facility and the vessels that operate from that facility, as long as the facility's security plan incorporates the vessel operations or the facility and vessels have separate approved security plans. Another commenter said that the use of card readers should be optional for facilities and vessels until experience is gained and best practices are developed within the industry.

One commenter requested that the final rule require that facility operators ensure that all readers deployed are fully functional and operational to ensure that all gates are accessible for truck drivers and other affected personnel to use.

Because the use of readers is not required by this final rule, concerns

related to the value or drawbacks related to requiring readers have been deferred. A more complete discussion of why recordkeeping requirements are no longer included may be found below in the section discussing recordkeeping requirements.

One commenter said that § 105.200(b)(8) requirements for adequate coordination of security issues between the facility and vessels that call on it are problematic for both passenger facilities and vessels. The commenter asked that the subparagraph be modified to reference only those that access secure or restricted areas, not the entire facility.

The referenced paragraph, while redesignated, was unmodified by the NPRM or this final rule and, therefore, no changes to the provision were considered.

One commenter said that the proposed rule does not adequately address a facility's responsibility to log seafarers off the ship and onto the facility for routine ship operations. The association asserted that the ship and its crew, by virtue of its clearance by Federal officials to enter port and begin cargo or passenger operations, should be considered a part of the facility and logging off the ship should not be necessary for either normal ship operations or access for shore leave.

Because the recordkeeping requirements have been removed from this rule, there are no specific TWIC logging off requirements. Removal of the TWIC recordkeeping requirements is discussed below.

One commenter stated that the rule must clarify that the owner/operator cannot be held responsible for events rendering employees ineligible for a TWIC of which the owner/operator has no direct knowledge.

Section 105.200(b)(14) establishes a responsibility on the part of the owner/operator to inform TSA of any information that he/she becomes aware of in the normal course of its operations or simply by chance. Whether the information is known "directly" or "indirectly," the intent is to ensure that facts, which would affect an individual's eligibility to possess a TWIC, are made available to TSA. The section does not impose a responsibility for an owner/operator to actively seek information on employees or other workers; merely to provide it to TSA should the owner/operator become aware of such information.

One commenter asserted that there is no discussion in the NPRM regarding how owners/operators should deal with a failure in the TWIC system other than to state that they must incorporate

backup processes into their plans. The commenter said that TSA and Coast Guard should provide some recommended alternatives. Another commenter expressed an interest in having consistency in the backup processes used by ports and urged TSA and Coast Guard to be more prescriptive on this matter.

One commenter noted the NPRM stated that if the TWIC reader breaks, security personnel should know how to compare the picture on the TWIC with the person's face or have someone vouch for that individual. The commenter then asked if matching a person's face to his or her picture is an acceptable approach to screening, why that method of screening is not an acceptable alternative to the readers more generally. Two commenters said that they supported the inclusion of language that allows operators to include protocols for responding to TWIC holders who cannot electronically verify a match between themselves and the information stored in the cards.

Because the reader requirement has been removed from this final rule, we believe that further discussion of what would constitute acceptable alternate security procedures should the TWIC system fail would be better addressed during a subsequent rulemaking that implements a reader requirement.

5. Requirements for Security Officers and Personnel

One commenter said that he would not have the time to attend any required training to become familiar with the TWIC program.

It is the responsibility of each individual to ensure that he or she receives all the training necessary to successfully perform his or her assigned duties. However, we will work closely with industry and other appropriate stakeholders to ensure that the knowledge requirements can be satisfied by all affected personnel.

One commenter stated that changes to §§ 105.205, 105.210, and 105.215 seem unnecessary because the proposed rule requires possession of a TWIC for unescorted access to a secure area.

We disagree; the provisions provide clarity and avoid any question as to the responsibility of Company Security Officers (CSOs) and other security personnel to have and maintain a valid TWIC.

One commenter asked whether the citizenship of a CSO would affect his or her ability to receive a TWIC. The commenter also asked whether the CSO and other security personnel of a foreign-flagged vessel would need to obtain a TWIC.

Foreign-flagged vessels, including cruise ships, and their crews are exempt from the TWIC provisions, as set forth in 33 CFR part 104. If the CSO is not a U.S. national or legally authorized to work in the United States, he/she may be eligible for a TWIC depending on whether he/she has applied for and received certain types of U.S. visas. We have expanded the eligibility for persons working under valid work visas to open TWIC eligibility to as many of these individuals as possible.

One commenter said that the proposed rule should be amended to provide the CSO with the authority to implement acceptable alternative screening measures for unescorted access to a vessel when the use of TWICs is impractical, unreasonable, and vessel security is not compromised. In particular, the commenter requested that the CSO be empowered with the discretionary authority to modify or exempt TWIC-controlled unescorted access and use the currently accepted procedure of a positive photo-identification along with verification from the worker's company.

Alternative Security Programs (ASPs), proposed and implemented pursuant to the existing regulations, will be available to owners/operators. The ASP must be approved pursuant to 33 CFR 101.120. We do not agree, however, with the proposal to allow CSOs the authority to accept alternative measures to TWIC without first obtaining approval for such an alternative from the Coast Guard. Provisions for seeking waivers or equivalents remain unchanged, and are listed in §§ 104.130 and 104.135, respectively.

One commenter noted that page 29403 of the NPRM refers to the "access control administrator of the vessel or facility." The commenter said that it already has a CSO, FSOs, and VSOs. It asked whether the NPRM would require companies to create a new position or assign a new set of duties to a company employee.

The term "access control administrator" was not intended to, nor does it, create a new position. It was used to describe a position that may or may not already exist at a vessel or facility. Additional duties to CSO, FSO and VSO are expressly set out in the Rule, and are not intended to overburden any of those positions.

One commenter asked how much knowledge of and training on the relevant aspects of the TWIC Program VSOs and other personnel of foreign-flagged vessels would be required to have.

Foreign-flagged vessels and their crews are exempt from the TWIC

provisions, as set forth in 33 CFR part 104. VSOs on U.S.-flagged vessels will need to know of those aspects of the vessel's TWIC Program that are relevant to his/her job. For example, if the VSO will be responsible for visually inspecting TWICs, he/she must be familiar with the security features of the TWIC, the alternative procedures to be followed when an individual tries to enter after reporting a TWIC as lost, damaged, or stolen, the procedures to be followed when a fraudulent (altered) TWIC is discovered, and the procedures to be followed when an individual without a TWIC tries to enter a secure area without escort.

One commenter noted that the NPRM proposed requiring that all individuals with security duties and those who may be examining TWICs at access control points have some familiarity with the security features of the TWIC. The company said that TSA or Coast Guard should provide an online course about the security features of the TWIC that can be completed prior to going to the enrollment center, at a kiosk, or at the enrollment center. Successful completion of that course would be required prior to the TWIC application being accepted. Another commenter suggested that the Federal government should provide more extensive outreach and direction to operators and Security Officers prior to finalizing the rule. The purpose of the outreach would be to receive input and to more fully discuss expectations of those who will be given new responsibilities by the rule.

We agree that further guidance on how to fulfill the training requirements contained in this final rule is necessary. The use of online courses may be implemented at a future date. In the interim, further guidance will be forthcoming through publication of an NVIC.

One commenter suggested that the CSO be provided with the option of activating TWICs on behalf of the enrollment centers. We are not considering this option currently, because it may introduce privacy and security issues with the security goals of the TWIC program. However, as the program develops, we will continue to consider ways to allow for greater flexibility in all levels of the program whenever appropriate.

6. Recordkeeping/Tracking Persons on Vessels/Security Incident Procedures

Sections 104.235, 105.225, and 106.230 of the NPRM proposed requiring Security Officers to maintain records for two years of all individuals who are granted access to the secure areas of a vessel, facility, or OCS

facility. Numerous commenters, including the SBA Office of Advocacy stated that, in general, the requirement is overly burdensome and would have no resulting security benefit. Several commenters requested a clear understanding of what this information will be used for and justification for the creation and maintenance of each of these records. A few commenters stated that this requirement is overly burdensome on cruise operators because of the volume of people coming and going. One commenter said that this requirement is especially burdensome on operators of small passenger vessels like water taxis but did not state why. Some commenters specifically asked that the requirement be deleted from the rule. Many commenters stated that two years is too long to maintain such records. In contrast, one commenter supported the two-year timeframe.

Many commenters noted that businesses that maintain security videotapes typically keep them for only a brief period. These commenters said that if no security incident has occurred relating to a particular entry to a secure area, there is no need to keep a record of the person involved. Should the Federal government need to "track" the presence of employees on vessels, it can obtain and rely on payroll records and other employee files typically kept in the course of business rather than imposing a mammoth new recordkeeping requirement?

Two commenters said that the recordkeeping requirement would further delay the processing of individuals in and out of port facilities, which would affect the flow of freight through the facilities. Five commenters said that the need to keep and access records would greatly increase operating costs.

One association noted that the requirement would force facilities and vessels to install both an entrance and an exit system and said that there have been technological problems with exit systems. It said that exit system technology should be tested before a requirement to use them is promulgated.

Two commenters said it is not clear by whom and where the access records would need to be kept for two years. One commenter suggested that the recordkeeping requirement would make more sense if it applied only to individuals picking up hazardous materials from their facility. A few commenters suggested that the rule be amended to allow video recording to meet the recordkeeping requirement. Additional commenters wanted crewmembers to be exempted from these general provisions to save on

paperwork, suggesting instead that crewmembers be logged into the system upon entry to the vessel and logged off upon final exit from the vessel without registering every entry and exit in-between.

Two commenters wanted vendor/contractor personnel to be entered into the database upon initial boarding and then entered again after his final departure. The commenters also stated that there is no need to record every trip made to and from delivery vehicles or shoreside offices/workshops.

Several commenters complained about the lack of personnel to maintain these records. They asserted that facilities will be required to manually enter information on visitors who are exempt from the TWIC requirement. Some commenters felt this was not practical. Two commenters wanted provisions added to the regulation to allow modified procedures for large work gangs, such as longshore gangs vetted by the port, to board the vessel to work cargo without each individual longshoreman being screened by the vessel prior to and at the conclusion of the workday.

Commenters balked at the amount of records that will need to be kept. Two commenters suggested that, to alleviate burden, the records should be automated through the TWIC system, which could keep track of all persons granted access to secure areas. This could be done through an additional access card. One commenter complained that the cost of readers is an unnecessary expense and does not need to be incurred for one-vessel or two-vessel operations, but that without the reader, the paperwork requirements become even more daunting. One commenter wanted the rule to specify exactly what information should be maintained and suggested: Name, ID number, and home address.

As noted above in the discussion of changes to the Coast Guard provisions, the recordkeeping requirements related to TWIC implementation have been removed from the final rule. We had proposed the requirements because we believed they could be satisfied by using the TWIC readers, which were also proposed. Due to our decision to remove the reader requirements from this final rule, it makes sense to also remove the recordkeeping requirements that were intrinsically tied to those readers. We will keep these comments in mind as we consider whether to re-propose new recordkeeping requirements.

Several commenters wrote in opposition to the requirement that vessel or facility owners ensure that

appropriate personnel know who is on the facility at all times.

One commenter said that the requirement would place a tremendous strain on many ports and would provide little value if individuals are properly screened during the entry process. According to the commenter, even if card readers are installed at each entry and exit point and all TWIC holders were to utilize them, provisions would still have to be made to capture data from visitors, vessel crew members, and passengers in freight trucks. The commenter noted that current Coast Guard regulations require ports to grant access to crew members of vessels, including foreign nationals. Because foreign nationals would not be eligible to obtain a TWIC, the port authority said it would have to hire additional security guards to escort crew members while they transit port property. The commenter added that the NPRM had not explained or justified the benefits of knowing precisely who is on a vessel or at a facility at all times or in requiring individuals to use a TWIC to exit.

Another commenter said the requirement would require readers at both entrance and exit gates and argued that exit control is costly and provides little additional protection. The commenter added that other industries have reported technological problems with exit systems. It noted that exit control is not required in the "higher risk" aviation sector.

One commenter said that it is not critically important to national security that facilities know exactly who is on a facility at any given time. It is only important to know that everyone on the facility has been cleared to enter. Another commenter said that this requirement would require every facility to construct a security building at every entrance and deploy security guards around the clock. The commenter said that the resulting compliance costs would be prohibitively expensive but would not improve the security of ports because facility operators are already guarding areas determined to be at risk.

Some commenters opposed the application of this requirement to passenger vessels. Two commenters said that because large cruise ships have hundreds of properly authorized visitors onboard at any given time, it would be unreasonable to require a single crew member to know who is onboard. They suggested that the ship's visitor and crew logs be utilized for this purpose because all cruise ships record the arrival and departure of each person while in port. A third commenter noted that passenger vessels can carry thousands of passengers and requested

that this requirement be drafted or explained in a way that could "reasonably" be applied to passenger vessel operations.

Another commenter recommended that owners or operators be required to know the whereabouts of contractors and visitors, but not facility employees. The commenter stated that it would be extraordinarily difficult to know who is present at a large facility with thousands of employees, because many people "badge in," but not out. The commenter said that the requirement as proposed could require new equipment at multiple access points with little enhancement of security.

Because the use of readers is not required by this final rule, these record keeping requirements and the requirement to know who is on a vessel or facility at all times have also been removed. Comments and concerns on these issues, however, will be considered in any subsequent rule which imposes a reader requirement.

One commenter requested that § 104.290(a)(1) and 105.280(f) be modified to conform to § 104.235 and 105.225, respectively, by requiring the availability of a list of persons who have been allowed access to secure areas, not to the entire vessel or facility.

Because the proposed record keeping requirements have also been removed, we have also removed the requirement that these records be made available after a security incident. Comments and concerns on these issues, however, will be considered in any subsequent rule which imposes a reader requirement.

7. Reader Requirements/Biometric Verification/TWIC Validation Procedures

We received a substantial number of comments on technology issues, almost all of which expressed concern about the feasibility and appropriateness of the proposed TWIC system. Commenters noted that the prototype did not test many parts of the proposed system including the readers and communications with a central database. Some questioned whether the central database is available. They questioned whether the systems will be compatible with existing systems; if they are not the cost of replacement will be high. Commenters stated that TSA must test the proposed system before requiring its use and ensure that it will work in the marine environment and that backup systems will function as well. They stated that if comprehensive testing is not done the result could be higher costs throughout the entire supply chain. In terms of interconnectivity, they stated that the

system has to be shown capable of processing 700,000 TWICs instantaneously. Commenters also noted that the system does not appear to have been tested with passenger vessels.

Many commenters stated that cards that had to be inserted into a reader would not work in the marine environment. These commenters stated that TSA had failed to demonstrate the contact readers would work reliably in the marine environment and had not accounted for the cost of frequent maintenance and replacement or the costs imposed by failures that delayed workers and cargo. One commenter noted that when it tested readers outdoors the device did not last five days. Many commenters recommended a contactless reader system as an alternative. They noted that this type of card was used in prototype. Commenters suggested that readers and cards should have mean time between failure of 10,000 hours and at least 6 months between maintenance.

Commenters stated that they needed to know what types of readers would be required before they could be reasonably asked to comment on the rule.

Many commenters questioned whether cost-effective fingerprint readers would work in the marine environment. They noted that the readers require clean screens and clean hands; the latter may be difficult in the marine and port environment. One commenter stated that one member using a biometric reader had a 300 percent annual repair rate, which meant that multiple backup systems will be needed.

Commenters stated that failure rates of 10 percent would have a serious effect on the ability to move cargo into and out of ports. One commenter noted that a failure rate of 10 percent would mean that 3,500 individuals a day would be delayed at LA/Long Beach. If 10 percent of trucks were delayed, the delay would ripple through the entire line of trucks waiting and through the supply chain. They recommended that an error rate must be less than one percent before the system is adopted. Commenters who had implemented biometric readers indicated that they had failed to perform satisfactorily.

After reviewing these comments, we have determined that implementing reader requirements as envisioned in the NPRM would not be prudent at this time. As such, we have removed the reader requirements from the final rule, and will be issuing a subsequent NPRM to address these requirements, instead requiring that the TWIC be used as a visual identity badge at MTSA-regulated

vessels and facilities. That NPRM will address many of the comments and concerns regarding technology that were raised in the above-summarized comments.

Many commenters opposed the requirement to install a TWIC reader on each vessel. One reason for this opposition was that crews on some vessels are small and very familiar with one another, making it difficult for an unauthorized individual to go unrecognized. Other commenters cited the high cost of installing readers on each vessel. Some commenters said that the readers would be difficult to mount on small vessels or would break down in the marine environment. Commenters also said that there is no legislative mandate to require TWIC readers on vessels. Some commenters suggested that the TWICs of vessel crew members could be scanned at the entry point to a facility prior to boarding a vessel.

One commenter said that alternative methods should be allowed for using the TWIC to vet personnel for access on board vessels without the use of readers. One alternative suggested by the company would be to allow all personnel to check in at a central location such as a company office, have their biometrics confirmed, and then be transported to the vessel via trusted agent. At the same time as personnel are being transported, a confirmed list of vetted personnel could be electronically transmitted to the vessel for confirmation purposes. Another commenter opposed a requirement for a TWIC reader on vessels carrying fewer than 150 passengers. A third commenter said that requiring all terminals, regardless of size and technological expertise, to have electronic readers and supporting IT systems in place and operating properly might further compromise efficient terminal throughput. If the readers and related IT systems don't function properly, they will exacerbate congestion and delays. The commenter said it is therefore essential that all technical and process-related issues are thoroughly ironed out before rules are finalized and the program is implemented.

As stated above, the reader requirements have been removed from this rule; therefore, it is not necessary to respond to these comments at this time. Concerns that remain relevant will be considered during the subsequent rulemaking.

One company said that each TWIC would include data on an individual's employer, which would mean getting a new TWIC after every job change. Because of the high turnover rate of

vessel personnel, the number of invalid TWICs would grow quickly.

Workers' eligibility to maintain a TWIC is not tied to his or her employer, and employer information is not included on the TWIC itself. Therefore, when a worker changes employment, TSA need not be notified, and neither the TWIC itself nor the individual's eligibility to hold and maintain a TWIC will be affected.

Some commenters pointed out the possibility that truck back-ups could occur or be made worse in the likely event that a truck driver arrives at a reader and finds that he or she does not have their TWIC or their TWIC is inoperable due to being damaged or some breakdown of the system. Another commenter expressed a similar concern about operational delays that could result from lost or damaged cards or system malfunctions during the typical rush of longshoremen arriving for work at or near the same time.

The removal of the reader requirements from this final rule should eliminate the concerns expressed above. Additionally, we have added specific provisions to accommodate persons who have reported their TWICs as lost, damaged, or stolen, to provide continued access for a limited time, until they are able to pick up their replacement TWIC.

Several commenters said that the requirement to check TWICs against an updated list from TSA would be overly burdensome, especially if the list of invalid TWICs becomes large. One company preferred that TSA establish a toll-free number and a website for checking the validity of a TWIC instead of requiring company to maintain a potentially large database. Another commenter said that TSA and Coast Guard should reduce the frequency of TWIC verification at MARSEC Levels 1 and 2. Alternatively, the commenter suggested that a company could maintain possession of a person's TWIC and verify them as frequently as necessary.

One commenter said that TSA and Coast Guard should be responsible to develop a system with which owners/operators can contact TSA to verify the validity of TWICs. The association said that one possible solution is to establish a web portal where facility operators, through a password protected system, are able to match a name and picture with the TWIC ID number.

Many commenters said that most vessels do not have Internet access and therefore would have trouble regularly updating their list of valid TWICs by downloading data from TSA. One commenter said it would theoretically

be possible to employ an agent at each port of call to physically deliver downloads to a vessel, but this would significantly increase the cost of the program. Another commenter noted that not all marine employers have computers, so there must be a way (*e.g.*, telephone-based system) for those without computers to check the validity of a TWIC.

One commenter noted that there are a number of areas on western rivers that are wireless dead zones. The company also noted that few existing vessels have satellite Internet connection capability and any such expectation should be included in the economic analysis. The commenter also added that if TSA and Coast Guard expect vessels to use landline connectivity, the cost to stop a vessel periodically (weekly or daily) to download the latest information to vessel card readers would be significant and should be included in the economic analysis.

Two commenters questioned whether satellite communications would remain available for civilian use at elevated security levels. One commenter said that at MARSEC 3, the Federal government takes control over communications satellites, thus making it impossible to download any data from TSA via satellite.

Several commenters said the proposed frequency for updating the TSA information used for TWIC screening is excessive. Several suggested alternative update frequencies for each MARSEC Level. Two commenters said the proposed update frequencies should be the same as for validation of HMEs (annually). A company involved in responses to marine spills said that the requirement to update its list of valid TWICs would be cumbersome and an extra burden during responses.

One commenter suggested that information about individuals who are determined to be a security risk should be communicated to the local Coast Guard for immediate dissemination to FSOs. The company argued that it would be "ridiculous" to require a time-sensitive industry to employ computers to search through millions of names in a national database to identify a name not on the list. The company said that national security would be better served by providing the much shorter list of "non-authorized" persons. One commenter requested that the rule clarify that a private regional entity under contract to a terminal operator would be allowed to maintain the database of valid TWICs for the operator.

Although a reader is not strictly necessary for checking the validity of a TWIC, in most cases, we believe that requiring facilities to manually check the validity of TWICs without including reader requirements is impracticable. Therefore, because the reader requirement has been removed from this rulemaking; the requirement that the credential's validity be checked against the TSA list of revoked credentials also has been removed. The Coast Guard, when conducting spot checks, will verify a TWIC's validity while confirming the identity of the TWIC holder. We will continue to consider ways to provide flexibility to owners/operators in satisfying this requirement in subsequent rulemakings.

One company asserted that TSA and Coast Guard had not provided any information to the regulated community regarding the size or format of the data files likely to be associated with the list of invalid TWICs. Without this information, the company said it could not provide detailed comments regarding the cost or difficulty in providing this information to its vessels or whether it is even possible with the systems currently in place.

We agree that this type of information is necessary for industry to effectively implement these requirements, and will keep this comment in mind as we draft our NPRM re-proposing reader and TWIC validation requirements.

One commenter said that U.S. vessels face connectivity issues when transiting foreign ports and would therefore not be able to comply with the proposed requirement.

We will keep this comment in mind as we draft our NPRM re-proposing reader and TWIC validation requirements.

Another commenter suggested that facial recognition should be allowed at MARSEC Level 1 instead of biometric verification. Another commenter asked what facilities would be required to do if there are delays in updating its database. The commenter said that this is a critical point, because many other high-priority actions would be taking place at MARSEC Levels 2 and 3.

These requirements have been removed from this rule and therefore, concerns related to the use of the credential at different MARSEC levels will be revisited in a subsequent rulemaking.

A commenter said that rather than placing the burden on employers to repeatedly check the validity of each worker's TWIC, the vessel or facility operator should have the option of registering its employees and others who access its vessels or facilities using

a TWIC with the Coast Guard. The Coast Guard would be responsible for notifying the operator if a TWIC it has registered has been invalidated.

As set forth in the NPRM, owner/operators could register its employee and others who access its vessel or facility using a TWIC with TSA, and TSA would notify the owner/operator if a TWIC is subsequently invalidated. TSA describes the process as "privilege granting." This process will still be available, even though we are not requiring owners/operators to routinely validate TWICs in this final rule.

One commenter questioned whether the Federal government would be able to update the list of invalid TWICs on a daily basis at elevated MARSEC Levels. Another commenter conjectured that if there is a terrorist incident that leads to elevated security measures, Internet and other communications systems would likely be taxed to the point of failure. This would make frequent updates of the TWIC database difficult if not impossible.

While it is impossible to predict with certainty how essential infrastructure will be impacted by a terrorist incident, we believe that the layered security approach imposed by the MTSA provides the best approach to ensuring the greatest protection to our maritime facilities. However, because the reader requirement has been removed from this rulemaking, so has the requirement that owners and operators check the credential's validity against the TSA hotlist. We will keep these comments in mind as we draft our NPRM re-proposing reader and TWIC validation requirements.

Several commenters said that the required scrutiny of TWICs should not change with the MARSEC Level. Commenters said that the card is designed to be secure and linked to the cardholder by biometric verification, so the security benefits of additional scrutiny would not be worth the effort. One association opposed the requirement that vessels download daily updates on the status of TWICs at MARSEC Levels 2 and 3. The association said that the proposed rule's discussion of MARSEC Levels was not based on reasonable risk analysis. One commenter said that the requirement for use of a PIN and daily check of TWICs at MARSEC Levels 2 and 3 would provide only a marginal increase in security that is not worth the time, effort, and potential problems these measures would create. Another commenter opposed the proposed requirement that all TWIC-enabled gates be manned at MARSEC Level 2, saying it would divert security resources when

they are most needed. One commenter said there is no history of legislative intent during the development of MTSA for a requirement that industry download latest TSA information during increased MARSEC Levels.

These requirements have been removed from the final rule and therefore, we defer any response to these comments. We will keep these comments in mind as we draft our NPRM re-proposing reader and TWIC validation requirements.

One commenter maintained that weekly/daily verification for maritime workers was unjustified based on the fact that hazardous materials truck drivers, who pose a greater security threat (due to operation by a single individual and close proximity to population centers and potential terrorist targets), are checked annually.

We believe that this commenter misunderstood what the NPRM meant by the weekly/daily verification, but note that the final rule does not include this verification procedure, and therefore we need not respond to it further at this time.

Some commenters stated that their facilities are not transportation facilities, and as such the cards will be used only to clear employees into the facility. They stated that their existing systems are sufficient and that shifting to the proposed TWIC would double the time required to process each employee, which could cause operational delays during shift changes. The TWIC system should be designed to be easily integrated into legacy systems or TSA should allow facilities to use their existing systems after an employee obtains a TWIC.

The NPRM was drafted to allow owners/operators to continue to use their existing access control systems so long as they were able to integrate the TWIC into those systems. The elimination of the reader, biometric validation, and card verification pieces from this final rule does not change this. In order to integrate the two systems, owners/operators will need to ensure that their own access control systems are updated to show whether the employee has a TWIC even when he/she presents only the facility-specific badge. In other words, an individual must still have a TWIC before he/she can be granted unescorted access to a secure area, even if the badge being used to gain entry on a day-to-day basis is not the TWIC.

The Navy stated that Department of Defense Common Access Cards (DOD CACs) should fulfill the TWIC requirements. As long as the DOD CAC is the official credential for the Navy, it

will meet the identification requirement in § 101.514(b) when required for official duties authorized by the Navy. If it is replaced with another credential in order to gain compliance with HSPD-12, however, that new credential will need to be used by Naval personnel seeking to gain unescorted access to a MTSA-regulated vessel or facility.

8. Access Control Issues

(a). New Hires/Persons Needing Access Before TWIC Is Granted

Many commenters remarked that seasonal workers are employed for 90 days or less, and those commenters believed that the rule would severely impede seasonal hiring if the workers had to wait 60 days for a TWIC. Some commenters pointed out that seasonal businesses often must find new or replacement staff quickly. An association noted that seasonal workers are generally students, who may not know where they are going to work 60 days before classes end. Another association described how a business might not have enough TWIC holders at the beginning of the season to escort the rest of the workforce.

We believe that the inclusion of the "employee access area," discussed above, should operate to exclude the vast majority of seasonal employees from even needing a TWIC.

Some commenters mentioned similar problems with short-term workers and casual labor hired with little advance notice, and those commenters described instances where workers are needed immediately. For example, in some businesses, deckhands come and go at a greater frequency than 30 days. One commenter remarked that it is not uncommon for a new hire to get onboard only to find out that they are not suited for work on vessels, leaving them scrambling to fill a position when a crewmember leaves. A State port authority noted that in addition to new hires, other individuals might need occasional unescorted access without having to wait for a TWIC card.

Several commenters objected to the fact that new hires would not be able to work until they obtained a TWIC card. Many other commenters agreed that the requirement would hurt the ability of companies to hire new workers and mentioned the high turnover rate in the industry, especially among entry-level positions. As one commenter described the situation, "When a worker needs a job, he or she needs a job now, not 30-60 days from now. If we cannot readily put people to work, there are any number of non-maritime employers who will be happy to hire them and put them

to work immediately." Commenters added that vessels and facilities would have to add security personnel to escort new hires and that TSA should develop some mechanism, such as temporary access, to address the period before the new hires or existing employees receive their TWIC cards.

One commenter had a suggestion for temporary access for visitors requiring unescorted movement for special cargo deliveries from a transportation mode not usually found in the maritime sector (e.g., oversized loads of equipment being shipped outside of the United States). A temporary TWIC should be established which can be granted by the facility after verifying two forms of identification and a check of databases. Various private companies already offer this service and DOD uses it for contractors and vendors to enter U.S. Army facilities.

Many commenters encouraged TSA and Coast Guard approval of a probationary period during which a new hire could begin work or training while the TWIC application is pending. Such a period could begin after the vessel, facility, or port has conducted its own background checks. Other commenters also favored a simplified or expedited background check (similar to those for firearms purchases) and interim, site-specific authorization for access. Some commenters specifically mentioned a temporary credential, similar to a temporary security clearance, or a pass authorized by the vessel or FSO. One commenter generally favored a shorter duration card.

A few commenters had suggestions about a different security system for short-term workers. One of them emphasized that casual laborers in the maritime industry may work for only one day, but casual laborers often outnumber permanent employees, so the requirement for escorts is impractical. One commenter added that the process required by the regulations must be flexible enough to allow small operators to respond to time sensitive demands for service, and cost-effective enough to allow these same small entities to continue to remain in business. Another commenter wanted to continue with its current photo ID system. A third commenter favored having annual renewal of the TWIC.

After reviewing these comments, we recognized the need to provide owners/operators with the ability to put new hires to work immediately if an urgent staffing requirement exists, once new hires have applied for their TWIC. We have included, above, a detailed discussion of the new provisions that have been added to this final rule to

allow new hires to have access to secure areas for up to 30 consecutive days, provided the security threat assessment process has begun, the new employee passes an initial TSA security review, and the individual remains accompanied while in the secure area. In addition, if TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may further extend a new hire's access to secure areas for another 30 days. Additional guidance on this provision will be forthcoming in a NVIC.

(b). Persons With Lost/Stolen/Damaged TWICs

Several commenters expressed concern that key personnel will lose their TWIC and not be able to enter a marine terminal or a vessel until they receive a new one. Several questioned TSA's estimation that replacement cards could be printed and shipped within 24 hours. One noted anecdotal evidence from participants in the Delaware River pilot that nearly two weeks elapsed before a replacement card was ready for activation. Another noted that the 24-hour estimation provided in the NPRM did not account for shipping time or the time required for an applicant to get to a TWIC enrollment center and that 3-4 days may be required for the entire replacement process. Many commenters indicated that it was important to ensure that individuals continue to access appropriate facilities while they await replacement cards or when they simply forget to bring their TWIC with them to work. Failing such access, operators will face burdensome work interruptions and employees might seek a different job or request unemployment compensation.

Commenters offered several suggestions regarding measures to mitigate delays that could result from lost, malfunctioning, or forgotten TWICs: (1) Temporary cards issued while an applicant awaits a replacement card; (2) some type of receipt indicating that the replacement card had been ordered; (3) providing a mechanism for a vessel/facility operator to capture the biometric from the card or from the TSA database for storage in the local database and validate an individual's identity by matching his fingerprint with the biometric stored in the local database in the event the individual leaves his card home on a given day; or (4) alternative identification verification provisions (e.g., visual identification, confirmation call to vendor's employer) included in vessel security plans for situations where mariners and shoreside personnel seeking unescorted access to the vessel have lost or forgotten their TWIC.

As noted above in the discussion to the changes to the Coast Guard provisions of this rule, we have added specific procedures for owners/operators to use to allow individuals to continue to gain unescorted access to secure areas for seven (7) consecutive days in the case of lost, damaged, or stolen TWICs. This procedure should alleviate the concerns over work slow downs or stoppages that were expressed by the commenters above.

One commenter noted a related issue that mariners whose TWIC is lost, stolen, or inoperable may have to be replaced on very short notice and that finding replacement workers could result in operational delays and other problems.

It is likely that the provisions added into the final rule, to allow for individuals with lost, damaged, or stolen TWICs to continue to work for up to seven (7) days, will alleviate this problem.

(c). Use of PIN

Several commenters objected to the requirement for TWICs to have an accompanying PIN number. Many of these commenters said the other security protections in the card would obviate the need for a PIN. In general, comments on this issue reflected two different interpretations of the proposed rule's requirement regarding PIN numbers. Some commenters assumed that the PINs would only be required at elevated security levels, while others assumed that TWIC holders would have to enter the PIN each time to unlock the biometric features of the card. One commenter opined on the treatment of PIN numbers in the FIPS-201-1 standard. According to the commenter, FIPS-201-1 states that the PIN must be validated before the two fingerprints stored on the card can be accessible. In addition, section 6.2.3 of FIPS-201-1 outlines the authentication steps, which indicate PIN validation occurs before biometric reading/validation. If this is correct, then the PIN will always be used since the NPRM proposes biometric validation when entering the secure area of a vessel or facility. Another commenter echoed these comments on the FIPS-201-1 standard and added that the requirement for use of a PIN regardless of threat level is inconsistent with "the MTSA philosophy."

Several commenters opposed the use of a PIN only at MARSEC Level 3. They said that because Level 3 occurs so infrequently, TWIC holders would probably forget their PINs. One commenter requested the use of facial comparison instead of a PIN for an

alternative means of identification. This commenter said that use of a PIN would compromise the security of the credential. Two commenters said that if PINs are required, there must be a way to check or reset a forgotten PIN within a very short period of time. Other commenters said that the use of a PIN would lead to long delays in access to port facilities and could disrupt the flow of commerce. Two of these commenters requested that the access system not lock out an individual after several unsuccessful attempts to enter his or her PIN, citing the potential resulting disruptions to the flow of commerce. One commenter said that a PIN entry pad will require additional maintenance (due to exposure to the elements) or additional infrastructure to make it immune to the elements (*i.e.*, enclosed boxes, protective barriers to prevent vehicles from contacting the box, etc.).

Because the reader requirement has been removed from this rule, the PIN requirement will not be an issue for routine access controls. We note, however, that the Coast Guard will be conducting spot checks for TWICs, using hand-held readers, and that if an individual is stopped during one of these spot checks, he or she will need to know the PIN in order to unlock the biometric stored on the card and allow for biometric verification. We are sensitive to those commenters who noted that, without daily use of the PIN, individuals will be likely to forget, however, as noted by some of the commenters above, having a card that is compliant with the current technology standard and provides the appropriate level of security and privacy requires the use of a PIN.

(d). Requirement That All Non-TWIC Holders Be Escorted

One commenter expressed concern about the impact of the escort requirement on visitors who do business at ports. The commenter noted that many port facilities may have normal deliveries (*e.g.*, mail, overnight delivery services) or businessmen and women visiting the port, and that ports should be given flexibility on how to handle these visitors. The organization suggested reviewing how the State of Florida handles visitors if it decides not to grant additional flexibility to facilities in the final rule, and said that the final rule should consider different escort requirements at different MARSEC levels.

Another commenter said that the escort provisions would be especially troublesome for small ports because of their limited security personnel. A third commenter expressed concern about the

resources that would be required to escort "one-time-only" drivers. A fourth commenter recommended that the type of escorting or monitoring required at Certain Dangerous Cargo (CDC) Facilities be based on a vulnerability assessment instead of dictated by standard, noting that additional information on risk could be incorporated from the Maritime Security Risk Assessment Model (MSRAM) or other assessment tools.

As explained elsewhere in this final rule, the term "escorting" has been broadly defined to allow flexibility to owner/operators, based on their individual operations, in satisfying the requirement. Further guidance as to how individual owner/operators can satisfy this requirement will be provided in a NVIC. We expect guidance will describe that when in an area defined as a restricted area in a vessel or facility security plan, escorting will mean a live, side-by-side escort. However, outside of restricted areas, such side-by-side escorting is not necessary, so long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual "under escort" be found in an area where he or she has not been authorized to go or is engaging in activities other than those for which escorted access was granted.

Two commenters noted that many technicians who work on shipboard equipment are not U.S. citizens. They typically work in areas of the ship that would not be considered public access areas and often work at night or when the regular crew is off-duty. The commenters maintained that vessel crews do not have the extra personnel to escort these technicians. One of these commenters requested that the final rule contain a provision for a foreign citizen to have access to vessels if they are approved by the ship's Master or Chief Engineer and recognized as a trusted worker.

We acknowledge that technicians who are non-U.S. citizens or immigrants are an integral part of the maritime industry. Lawful nonimmigrants with unrestricted authorization to work in the United States may apply for a TWIC. In addition, we are amending the immigration standards to permit foreign nationals who are students of a State Maritime Academy or the U.S. Merchant Marine Academy to apply for a TWIC. Also, we are permitting certain aliens in the United States on a restricted work visa to apply for a TWIC. Applicants sponsored by a U.S. company authorized to work on a temporary basis in the United States under an H visa, individuals employed in the United

States on an intra-company transfer under an L visa, NAFTA professionals in the United States under a TN visa, nationals of a country that maintains a treaty of commerce and navigation with the United States and is engaging in substantial trade under an E-1 visa, is in or is coming to the United States to engage in duties of an executive or supervisory character under an E-2 visa, applicants with extraordinary skill in science, business, or art entering the country on an O visa, and Australians in a specialty occupation under an E-3 visa are now authorized to apply for a TWIC. The companies that hire these individuals are required to notify TSA when the workers are no longer employed at their U.S. operations, recover the TWIC, and return it to TSA. In addition, the rule requires the workers to surrender the TWIC to the employer when leaving that place of employment in the United States. We are requiring the surrender and retrieval of the TWIC to prevent instances in which a worker would hold a 5 year TWIC, but be authorized to work in the United States for a much shorter period of time.

One commenter said that the escort requirement, when combined with other requirements in the proposed rule, could have the side effect of completely dismantling what remains of the U.S. Merchant Marine. The commenter said that companies will only flag their ships in the United States as long as there is an economic incentive for them to do so. The commenter maintained that the cost of providing TWIC-carrying escorts for all foreign citizens, purchasing the necessary equipment, and paying for more training could motivate companies to flag their ships under another country's flag.

We share concerns about unintentional negative impacts TWIC implementation could have on the maritime industry. Where the governing statutory provisions provide the Department with discretion, we continue to weigh the security benefits of implementing TWIC against the burden it imposes upon industry. We believe that the provisions set forth in this final rule reflect a reasonable implementation that will not overly burden industry and we will continue to evaluate the impact on industry as we proceed with future rulemakings.

One commenter expressed concern about how maritime ministry activities would be affected by the implementation of the rule.

The Coast Guard supports the activities of those organizations providing services to seafarers of all nationalities. Chaplains and other

humanitarian workers are encouraged to obtain TWICs and to work with owner/operators in preserving continued unescorted access to vessels and seafarers.

(e). Vessel-Specific Issues

Coast Guard proposed adding § 104.106 to provide for passenger access areas on board passenger vessels, ferries, and cruise ships, which would allow vessel owners/operators to carve out areas within the secure areas aboard their vessels where passengers are free to move about unescorted. Many commenters supported this provision and stated that these concepts are absolutely essential to a workable rule. The commenters argued that without this provision, the passenger vessel industry, which depends on attracting the public as customers, would not be able to function. Several of the same commenters stated that the clarification that a vessel employee whose duties require unescorted access to a passenger access area, but not to secure areas of the vessel, would not need a TWIC needs to be explicitly stated in the language of the final rule.

Some commenters wanted clarification of the different types of areas on a vessel. One commenter was unable to determine whether all areas not designated passenger access areas are to be considered "secure areas." The commenter noted that, using the definition of passenger access area as found in proposed § 104.106, a passenger area would not necessarily be within the access control area or "secure area" of a vessel or facility, which seems to be a contradiction as it is written in the proposed rule.

As defined in § 104.106, passenger access areas are located within the access control areas of the vessel (and are thus within the "secure area"), but by definition they are not part of the secure area. They can be thought of as pockets within the secure area—all areas around the passenger access areas are secure and require TWICs for unescorted access, but the passenger access area does not. As such, any employees whose duties keep them entirely within the passenger access area do not need a TWIC, the same way that passengers would not.

Some commenters also noted that certain vessel spaces are absolutely essential to security (*i.e.*, the bridge and the engine room), adding that the current MTSA regulations use a definition of "restricted area" that implies that only certain portions of a vessel will be so designated.

We agree that only certain portions of the vessel need be designated as

restricted areas. As noted above in the discussion of the definition for secure area, we considered requiring TWICs only in these areas, but determined that doing so might actually be more harmful to owners/operators. The NPRM included reader requirements, including the use of the TWIC and readers for biometric verification. Using the restricted area as the secure area would have required that these readers and the verification be used at the entry points of each restricted area. This would have likely meant that many vessel owners/operators would have needed more than one reader, increasing their compliance costs. Additionally, the process of biometric identification could have interfered with the operation of the vessel. As a result, we decided to define the secure area as the access control area, thus limiting the number of readers required, as well as the number of times biometric verification would need to take place.

This final rule does not include the reader and biometric verification requirements, but we do expect to issue a second rulemaking in the future that will re-propose these requirements (although they may have some differences from what was included in the NPRM of May 22, 2006). Because we expect to require readers and biometric verification in the future, we do not think it is a good idea to confuse the maritime industry by adopting a definition of secure area in this final rule that would not be workable when reader requirements go into effect. As such, we did not revise the definition of secure area to coincide with the restricted areas.

One commenter requested clarification that for foreign-flagged cruise ships, the Flag State-approved and ISPS Code compliant Ship Security Plan (SSP) is where passenger access issues would be discussed. The commenter wanted confirmation that no additional plan, such as the TWIC Addendum described in proposed § 104.115, or revision to existing plans is necessary for foreign flag cruise ships under either of these regulations.

For reasons discussed above, § 104.105 exempts all foreign-flagged vessels, including foreign cruise vessels, from TWIC requirements.

Another commenter noted that the creation of § 101.514 does not address the existence of a "passenger access area" as an exception, and the language of § 104.100 needs to be referenced here with other exceptions to having a TWIC. Therefore, the commenter suggested that a new subparagraph should be added to read: "No passenger, employee, or other individual needs to possess a TWIC to

obtain unescorted access to a passenger access area as defined in § 101.106 or a public access area as defined in § 105.106.”

We do not agree with the suggested change. Because the definition of passenger access area clearly states that these areas are not secure areas, it is clear that TWIC requirements do not apply within the passenger access area.

One commenter stated that contractor personnel working for oil and gas operators on vessels would be required to carry a TWIC or be escorted on the vessel. The commenter concluded that, with up to 36 oil field workers on a vessel, this would put a strain on the crew to escort the individuals without a TWIC.

This is technically correct, however we hope that the clarification of what was meant by “escorting” will alleviate these concerns and any additional strain on vessel crews. In our clarification, we expect that when in an area defined as a restricted area in a vessel security plan, escorting will mean a live, side-by-side escort. However, outside of restricted areas, such side-by-side escorting is not necessary, so long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual “under escort” be found in an area where he or she has not been authorized to go or is engaging in activities other than those for which escorted access was granted.

One commenter noted that the proposed rule does not address how to handle access control and identification on vessels under repair in shipyards or in drydock. The commenter suggested that the rules should specifically address this issue and state that the owner of a vessel that is withdrawn from navigation, whether permanently or temporarily, is not required to implement or maintain access control and identification requirements while the vessel is not in navigation.

The MTSA regulations already state that vessels that are laid up or out of service are not subject to part 104. This applies to vessels no longer anticipating MTSA operations. For vessels that are undergoing repairs of a temporary nature, they must be in compliance with their approved VSP including access control measures. However, the approved VSP may contain security measures for intermittent operations, such as drydocking and shipyard repair work. These intermittent security measures may include relaxing access control measures during repair periods, but will include specific measures to reestablish access control and monitoring of the vessel and conducting a sweep of the entire vessel to ensure no

unauthorized objects have been left aboard.

Referring to proposed § 104.265(c)(4), one commenter stated that this requirement implies that a MODU vessel with several restricted (secured) areas, would be required to have a card reader at the entrance to each of these areas. The commenter argued that the vessel should only be required to have a card reader at the point(s) of embarkation to the vessel. Additionally, the commenter stated that the vessel would incur undue burden to ensure that a person trained in the TWIC to be assigned/posted at the entrance to each secure area and verify the TWIC for these people.

This comment displays a confusion regarding the meaning of secure area. It is not to be read as meaning the same as restricted area, but rather to coincide with the access control area of the vessel or facility. In the case of a MODU, this would be the entirety of the vessel. Additionally, the MTSA regulations allow for the checking of identification at the point of embarkation to the MODU, and the TWIC provisions do not change this.

One commenter supported proposed § 104.265(c)(8), which permits coordination, where practicable, with identification and TWIC systems in place at facilities used by vessels. The commenter recommended further broadening these provisions to clarify that when a vessel is berthed at a facility which is required under part 105 of these regulations to have a TWIC system in place, the vessel may suspend its TWIC operations while berthed at that facility. The commenter argued that there is simply no need to require duplicate TWIC validation especially when considering that facilities and vessels already have other non-TWIC security and access procedures in place.

We do not agree with this comment; the vessel owner/operator must maintain the ultimate responsibility for the security of his or her vessel. Amending the regulations as the commenter suggests would shift that ultimate responsibility to the facility owner/operator without requiring a contractual relationship with the vessel, which is inappropriate.

(f). Facility-Specific Issues

A law firm representing six companies suggested the following technical change to § 105.255(a)(4): “change the word “Prevent” to “Deter” to be consistent with the rest of the maritime security regulations.”

We disagree with this recommendation. Owners/operators must ensure the implementation of

security measures to prevent an unescorted individual from entering an area of the facility that is designated a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area.

The same law firm requested a clarification of § 105.255(d), asking “what is the meaning of the phrase ‘complies and is coordinated with TWIC provisions.’”

This provision allows the facility owner or operator to use a separate identification system, but it must be in addition to the TWIC. Requiring coordination means that the separate ID system cannot be used if it would allow someone without a TWIC to get unescorted access to secure areas.

We received one comment on the requirement proposed in § 105.255(c) (3) for facility operators to ensure that the facility operator’s TWIC program “uses disciplinary measures to prevent fraud and abuse.” The commenter stated that this would not be the correct assignment of responsibility, because the relevant evidence is only in the possession of government. The commenter also stated that the TWIC is a federally-issued credential obtained by an individual without the involvement of a facility operator or employer. If a TWIC is fraudulently obtained and used or abused in some manner, that would be a serious matter to be addressed by Federal law enforcement and not a subject for employer-imposed discipline. The commenter contended that the employer would not have the necessary evidence to impose discipline under the regulations.

The existing regulations already required owners and operators to have disciplinary systems in place to enhance the legitimacy of their identification system, whether it was a facility issued badge or a State-issued identification credential. There is a difference as to what the disciplinary system would be in each case, but we do not think it is inappropriate to place this responsibility on the owner/operator. For example, the facility owner or operator could fire and possibly take legal action against someone for tampering with the company’s badging system, but if they found someone presenting a suspected fake ID, an appropriate disciplinary measure could be to deny access, and could even go as high as firing the individual. Similar disciplinary measures can be put in place in regards to TWIC.

One commenter noted that § 105.255(f)(4) implies that vessel crew and others seeking access to a vessel via a facility, who do not have a TWIC, fall under the definition of “any person”

when visiting a facility. The current version of this section, § 105.255 (e)(3), reads “vessel passengers and crew,” while the above-proposed wording eliminates the word “crew” from the section.

The phrase “vessel personnel and crew” was removed and replaced with “any person” to clarify that the world of persons without a TWIC who might need access through a facility to a vessel is bigger than just vessel personnel and crew. If, however, the vessel personnel and crew do have a TWIC, they would no longer fall into this category of “any persons,” but rather into the separate category of persons with TWICs.

Some commenters argued that the proposed regulations are unclear about whether the currently accepted forms of seafarer identification are considered “government identification.” One commenter noted that the Coast Guard’s section-by-section analysis to § 105.255 reads that persons presenting for entry who do not hold a TWIC would still be required to show an acceptable form of identification, as set forth in §§ 101.515 and 104.265(e)(3). Current Coast Guard guidance states that passports, seaman’s books, STCW endorsements, and driver’s licenses are acceptable forms of identification that a foreign mariner could use to access a facility. The commenters proposed that the Coast Guard either add the existing approved documents contained in current Coast Guard guidance to the list of acceptable items in proposed § 105.255(f)(4), or clarify in the comments to the final rule that existing approved documents are still acceptable as “government identification” so long as they comply with proposed § 101.515. The commenters also suggest the Coast Guard add “crew” or “crew of a foreign vessel” into the list of non-TWIC holding personnel referenced in proposed § 105.255(f)(4).

The list of documents found in § 105.255(f)(4) are intended to be used to verify an individual’s reason for accessing a facility. The inspection of these documents should be read in conjunction with the general requirement to check an individual’s identification by examining an ID meeting the requirements set out in § 101.515. We have not amended either §§ 105.255 or 101.515 to specify that the items listed in the Policy Advisory are adequate, but we have no intention, at this time, of changing that guidance.

One commenter also recommended the revision of 33 CFR 105.255(b)(1) to read “Each location allowing means of access to designated secure areas on the facility must be addressed.” The commenter stated that as currently

worded, this subparagraph contradicts 33 CFR 101.105, 33 CFR 105.225(b)(9) and 33 CFR 105.255(a)(4), subparagraph (c)(1), and could be misinterpreted as requiring that a facility’s access control program cover a much more extensive area than is the intent of the proposed regulations.

This final rule will no longer be adding language to this paragraph, therefore the suggested change is no longer necessary.

One commenter noted that at small ports, it is the terminal operator’s responsibility to ensure compliance with the security plan and that many small ports face a tremendous difficulty in doing the “people” side of security. Another commenter stated that port facilities should be given more flexibility regarding escorting of visitors.

We appreciate the concerns raised by the commenters, and have provided clarification elsewhere in this final rule as to what is meant by “escorting,” which we hope will alleviate these concerns.

One commenter raised the question of whether family members traveling with truck drivers in the summer would be required to have an escort in secure areas of marine facilities. They pointed out that many truck drivers travel with family members in the summer months.

In accordance with the access control provisions of both the NPRM and the final rule, owners and operators of facilities are required to check identification of all persons prior to granting access and to require a TWIC prior to granting unescorted access to secure areas. In the case of family members traveling with authorized personnel who require unescorted access to secure areas of a facility and also hold a TWIC, it remains the responsibility of the owner or operator to continue to either allow the authorized personnel to serve as the escort for their family member, or to follow the same procedure used for any other visitor that does not hold a TWIC.

Some comments proposed that current security programs or credentialing programs should be evaluated as an alternative to the proposed rule.

The MTSA regulations in 33 CFR parts 101, 104, 105 and 106 provide for acceptance of ASPs, waivers, or equivalents. These provisions still apply, even with the addition of the TWIC requirements. Note, however, that they would only apply to the facility owner/operator’s access control responsibilities; they would not alleviate an individual’s burden to apply for and obtain a TWIC if they

require unescorted access to a secure area.

One commenter said that a universal identification credential such as TWIC, should allow mariners unescorted access to the terminal when there is a valid need for such access, *i.e.*, to reach the job site aboard a ship berthed within the port facility. Indeed, the mandatory provisions of the ISPS Code (ISPS Code—Part A Requirement 16 Port Facility Security Plan) require such facilitation of access by mariners. The commenter stated that owner/operators, in complying with the proposed rule and with approved security plans, should be sufficiently reassured (for liability purposes) to allow unescorted access to the TWIC holders with a legitimate need for admittance, and that the proposed rule should make clear that owners/operators of secure areas who follow their approved security plan and who adhere to the TWIC access control procedures will not be deemed liable for some type of breach unforeseeable within the federal port security regulations.

We agree that possession of a TWIC should serve as evidence that a mariner does not pose a security risk to a facility owner, and that facility owners should be able to rely upon this fact in allowing mariners unescorted access through their facilities in order to facilitate crew changes, take shore leave, or complete a variety of other duties that may require the mariner to step off of the vessel onto the facility. Issues of liability are beyond the scope of this rule.

A commenter expressed concern about how it would implement the proposed rule at its fenced port facilities, where access control is handled by security officers who check the identification of everyone who drives in. The commenter said it did not seem practical to have employees use a card reader just to drive in past the security officers. The company also said that the restricted areas of its facilities are not enclosed spaces that can be locked off, so card readers would not work to control access to them.

While card readers are not required by this rule, owner/operators remain responsible for controlling access to restricted areas in accordance with existing regulations. Additionally, it is noted that the definition of secure area is not the same as restricted area, as explained elsewhere in this final rule. This final rule imposes a responsibility on owner/operators to ensure that only TWIC holders are allowed unescorted access to secure areas. While satisfying the escorting requirement for individuals without a TWIC may be accomplished by other means than

requiring a side-by-side escort in some secure areas, this final rule requires that owner/operators ensure that access to restricted areas by individuals without a TWIC is only allowed while in the presence of at least one TWIC holder.

One commenter said that it is necessary that the rule put the eventual TWIC holding population on notice that they will require a specific, discrete authorization or a "business purpose" when seeking access. The company requested that the final rule restore language that is currently in 33 CFR 105.255(e)(3). That language clearly requires that the reason for access be checked as a routine part of access control. The company said that this requirement is an important and essential layer of access security and affirms the requirement in 33 CFR 105.255(a)(4). The company added that this requirement has been muddled and diminished as the requirement for asserting business purpose when seeking access found at 33 CFR 105.255(f)(4) now only applies to persons not holding a TWIC and seeking entry.

Section 105.255(a)(4) clearly establishes the requirement that individuals may only be allowed unescorted access if they: (1) Have a valid TWIC and (2) are authorized to be in the area pursuant to the facility security plan.

(g). Outer Continental Shelf (OCS) Facility-Specific Issues

Some commenters referenced proposed § 101.514, the general requirement that "all persons requiring unescorted access to secure areas of vessels, facilities and OCS facilities, regulated by parts 104, 105 or 106 of this subchapter must possess a TWIC. . . ." One commenter stated that this requirement should either be removed from this section and placed individually in parts 104, 105 and 106, or a specific and limited exemption provided for certain vessels regulated under part 104. One commenter said strict adherence to the TWIC requirements is not feasible for off-shore foreign vessels routinely operating on the U.S. OCS. One commenter said § 101.514 is a particularly onerous requirement for newly hired personnel to work on a U.S. flagged mobile offshore drilling units (MODUs) and do not possess a TWIC. Another commenter stated that these limited exemptions should include U.S. flag MODUs and offshore supply vessels (OSVs) because the vessel manning statutes specifically recognize the necessity of permitting these vessels which are operating outside the

geographic boundaries of U.S. jurisdiction to employ non-U.S. citizens and immigrants in their crews. The commenter noted that MODUs in particular are often required to employ indigenous labor as a condition of operations on the continental shelf of another nation, and it is difficult to envision a scenario under which these non-citizens could present a security threat to the United States. Similarly, the commenter notes that the manning statutes recognize that non-citizens should be permitted to fill the vacancies created when a vessel sailing foreign is deprived of members of its required complement. The commenter concluded that it is simply unreasonable to expect that an escort with a TWIC can be provided for either a watchstanding member of the crew of an OSV for the duration of a voyage, or to an industrial worker on a MODU for the duration of a foreign drilling contract.

One commenter stated that strict adherence to the TWIC requirements of this part is simply not feasible for vessels routinely operating outside the United States. The commenter argued that application of the requirements, as proposed, would render it impossible to operate a U.S. flag MODU or OSV in foreign waters, would make it impossible to affect repairs in a foreign shipyard, and would negate specific provision of the manning statutes that permit the employment of non-citizens in specific circumstances. Therefore the commenter recommended that the proposed § 104.105(d) be revised to read as follows:

(d) the TWIC requirements, including those related to unescorted access, found in this chapter do not apply to:

- (1) foreign vessels;
- (2) U.S. vessels employing non-citizen crewmembers under the provisions of 46 U.S.C. 8103(b)(3) or (e), with respect to those crewmembers;
- (3) U.S. MODUs, offshore supply vessels or other vessels engaged in support of exploration, exploitation, or production of offshore mineral energy resources operating beyond the water above the Outer Continental Shelf (as that term is defined in section 2(a) of the Outer Continental Shelf Lands Act (43 U.S.C. 1331 (a)).

As noted above in the discussion of the changes to the Coast Guard provisions of this rule, we are adding a provision to the definition of secure area in § 101.105 that states that U.S. vessels operating under the waiver provision in 46 U.S.C. 8103 (b)(3)(A) or (B) have no secure areas.

We are sympathetic to the concerns of OSV owner/operators, whose vessels are required to comply with part 104 but are

transporting crew members to MODUs that are not subject to part 106, and therefore will not have TWICs. We believe that the clarification of the term "escorting" should provide some relief to these owner/operators.

One commenter noted that the proposed rule states that foreign vessels entering U.S. ports that carry a valid ISPS Code certificate are deemed to be in compliance with part 104, except §§ 104.240, 104.255, 104.292, and 104.295. And, under § 104.105(d), the proposed rule exempts all foreign vessels from the TWIC requirements. Several commenters requested confirmation that the combination of the exemption of foreign vessels from the TWIC requirement and the existing acceptance of ISPS certification for foreign vessels excludes an OCS facility which is a foreign-flag MODU "on location" from the TWIC requirements. The commenters also requested confirmation that there would be no TWIC requirements for a non-covered MODU working next to or over a covered OCS facility. Another commenter, seeking clarification of the proposed rule, asked: If you have a voluntary compliance for a MODU and it obtains a flag-issued International Ship and Port Facilities Security Code certificate, is that sufficient for exemption from TWIC requirements?

A foreign-flag MODU "on location" in U.S. waters and holding valid ISPS certification would be exempted from the TWIC requirements of parts 104 and 106.

One commenter believed the escort rules were unreasonable for the oil and gas industry and anticipated that these rules would lead to company and service personnel needing to obtain a TWIC.

The clarification to the escort provisions, provided elsewhere in this final rule, should alleviate the concerns of this commenter by limiting the need for live accompaniment to those instances where the company/service personnel are in restricted areas. At all other times, monitoring would be acceptable.

(h). Other Issues

Many commenters said that the rule should give owners/operators of vessels and facilities the ability to use the TWIC as a "visual identity badge." Some commenters specifically advocated visual checks of TWICs at MARSEC Level 1. Another said that TWICs could be used as a visual identity badge in the early stages of implementing the rule and could be used with readers after more experience is gained with the reader technology. One association

asked that passenger vessels and facilities be allowed to employ TWICs as visual identity badges and not be required to install readers.

Several commenters found fault with the statement in the NPRM that "allowing owners/operators to rely solely on the visual identity badge system is unreasonable in light of the additional cost of the credential, and the available security enhancements that the increased cost represents." These commenters did not think the requirement to use TWICs with biometric readers should be justified by the cost of the TWICs themselves. One commenter noted that TSA officials have endorsed the use of a visual identity badge system for airport employees and said that if such a system is sufficient for the aviation sector, it should also be used in the maritime sector. A shipbuilding and ship repair company argued that a visual identity badge system is needed to prevent delays as hundreds of employees arrive for work.

As already noted, this final does not address reader requirements. However, owners and operators may choose to use the TWIC with an existing physical access control system. The hotlist will be available to owners and operators who could use the magnetic strip or the cardholder unique identifier (CHUID) embedded in the credential to tie it into a legacy system that checks those entering against the hotlist. Although this option is available for owners and operators, the use of reader technology is not required at this time. We will revisit concerns related to other uses of the TWIC in the subsequent rulemaking.

Commenters found access control regulations for train workers within the current TWIC proposal unclear. One commenter recommended that rail facilities be allowed to check workers before boarding a port-facility bound train; another was unsure if train operators would require a TWIC and how other rail worker access control issues should be handled by the industry. Similarly, another commenter noted that train crews pose a unique problem because they enter maritime facilities on trains proceeding down the track. Trains do not typically stop at the property line of maritime facilities, and there is no guard house at which the train crews can scan their credentials. The commenter recommended that railroads be permitted to check crews before they get on the train.

Rail workers will require TWICs if their job requires them to have unescorted access to secure areas of maritime facilities. How and when those TWICs are checked is a process for the

train operator to work out with the facility owner/operator, in accordance with the latter's FSP, but the baseline requirement is that unescorted access not be granted to secure areas without a TWIC.

Commenters complained that the proposed rule reflects a "one size fits all" approach and did not take into account the different levels of risk and vulnerability across the maritime industry. Several commenters said that the proposed rule should be reviewed to assure that it is both risk-based and incorporates performance-based standards as much as possible. One commenter noted that most programs implemented under MTSA have thus far relied upon risk-based standards, but that the proposed TWIC rule is based on a "one size fits all" formula that applies the same security rules and the same costs to all operators. The association said that the broad application of this approach could prove to be an undue hardship for smaller and less threatened terminals and facilities that do not have access to the same resources as larger facilities. The commenter suggested that TSA and Coast Guard consider whether a risk assessment could be incorporated into the TWIC program, where practical, to minimize any disadvantage or undue adverse impact on smaller marine facilities.

Some commenters noted that the "Low Consequence Facility" designation allows the COTP some flexibility in determining how to logically secure the port without burdening industry with unnecessary requirements that produce no viable improvement in terrorism-related security. The commenters asked TSA and Coast Guard to incorporate the "low consequence facility" designation into the regulations.

Another commenter similarly requested alternative facility-specific identification systems for "low-risk operations." Another commenter said that a risk/vulnerability assessment would result in more vessels and facilities being exempted from the TWIC requirement. As an example, he suggested that the cut-off for vessels would be between 500 and 5,000 gross tons. Two commenters said that they did not consider the proposed rule to be tailored to specific and realistic security threats facing the inland marine transportation industry. Another commenter said that requiring card readers for low-risk business operations would be unreasonable and unproductive. The company also said that tow operations would be susceptible to armed takeover attempts even with a TWIC requirement in place,

so the rule would not provide any security benefits to these operations.

The MTSA regulations are inherently risk-based, as only those facilities and vessels determined to be at risk of a TSI were included in the applicability of subchapter H. The TWIC regulations intended to provide flexibility to owner/operators through the submission and approval process of their individual TWIC Addenda and security plans. Because many of the "one size fits all" requirements have been removed from the final rule, we defer a more specific response until our subsequent rulemaking on reader requirements. We will keep these comments in mind as we draft our NPRM re-proposing reader and TWIC validation requirements.

Many commenters said that the proposed rule would cause unreasonable delays for people attempting to enter facilities. Commenters often said that the resulting delays would disrupt or slow the flow of freight through U.S. ports. One commenter referred specifically to employees who move in and out of facilities several times a day. They expressed concern about these employees having to do a biometric verification each time they re-enter the facility. Several commenters said that the delays caused by the proposed rule would result in increased air pollution, because trucks would idle longer while waiting to enter port facilities.

Commenters said that the proposed rule would drive up the cost of goods that are shipped through ports, which would drive business away. One commenter stated that the proposed rule would pose a potentially significant barrier to international trade. Another remarked on the importance of the Port Authority of New York-New Jersey to the regional economy and the need to minimize disruptions to its operations. A commenter predicted that the rule's impacts on port operations would have secondary effects on industries that rely on imports. One commenter said that the cost of complying with the proposed rule would increase the cost of U.S. exports, reducing the competitiveness of American companies in the global marketplace. Another commenter said that the cost of complying with the proposed rule would hurt the competitiveness of U.S.-flagged ships.

The Department understands that this rulemaking imposes costs on businesses. The Department believes that those costs are a product of statutory mandates and the Nation's security needs. We refer readers to the accompanying Final Assessment for further details on our assessments of the costs and benefits of this rule. This

should assuage concerns arising from the use of the TWIC as set forth in the NPRM. We will revisit concerns related to other uses of the TWIC in a subsequent rulemaking.

One commenter requested that the final rule specify that no port facility or vessel may require the visitor or worker to give up possession of their TWIC as a basis for entry. Any handling of the card by anyone other than the cardholder should be limited strictly to the immediate task of processing the card in a reader, and the card must be promptly returned to the holder unless it has expired or been flagged for revocation.

We agree with this comment as it relates to the final rule issued today. We are aware of several facilities that use their own badging system, and as part of that system they require visitors to leave a form of personal identification with a security officer before they are able to receive a facility specific badge. These systems have largely been approved by the Coast Guard. However, we do not think it is appropriate for these visitors to be required to leave their TWIC behind if they have another form of identification they can leave (e.g., drivers license) after the TWIC has been visually inspected.

One commenter said that the original intended purpose of the TWIC was to facilitate access to secure vessels and facilities for those with the right to obtain such access. The commenter said that the original intent did not include denying access to those without a TWIC.

We partially agree. While facilitating access was one intended result, it also had the purpose of increasing security at our nation's ports by identifying those individuals who would receive unescorted access to secure areas. While the regulations do not prevent an owner/operator from granting access to individuals without a TWIC, they are now required to ensure that an individual without a TWIC is either escorted or is not allowed to enter secure areas.

Some commenters said that the rule was written for "blue water" ports and oceangoing vessels but would not work well for the off-shore energy sector or the inland towing industry. Other commenters said that the proposed rules appear to have been developed with little appreciation for the operational realities of the American tugboat, towboat and barge industry.

Many of the concerns expressed regarding the TWIC implementation as proposed by the NPRM should be assuaged by deferring TWIC reader requirements to a subsequent rulemaking. We believe that if further

flexibility is required in implementation by a particular industry or operation, the waiver and ASP provisions that currently exist in the regulations can provide it.

One commenter recommended that the rule allow facilities to store biometric information from the TWIC in a facility database with the individual's permission. This option, exercised at the discretion of the facility, would allow the facility operator to validate an individual's identity by matching the fingerprint with the biometric information stored in the facility database in the event the individual leaves his or her card at home on a given day. Local controls could be written in the FSP, and approved by the Coast Guard, to prevent abuse of this option.

One commenter wants DHS to grandfather facilities that have installed new access control systems within the last three years so they will recover their costs in implementing them.

Many expressed concerns that the TWIC would displace sophisticated access control systems already in place at regulated facilities. Many suggested that facilities that had invested significant amounts of capital into access control systems be allowed to continue using those systems in conjunction with TWIC. Others suggested that facilities be allowed to use alternate systems in place of TWIC.

TWIC technology can be adapted to existing access control systems, and it was not our intent to force owner/operators with sophisticated systems to abandon those systems to accommodate TWIC. We believe that TWIC enhancements can be fully integrated to most existing physical access control systems, and hope that the language of the final rule clarifies that owner/operators need not replace existing systems so long as TWIC capabilities are appropriately incorporated into the facilities' existing system. A NVIC providing further guidance on applying the access control requirements in this final rule is forthcoming.

9. TWIC Addendum

One commenter said that the time allowed for completion of a TWIC Addendum should be at least one year. The company based this request on the complexity of the proposed program, especially for shipyards that must coordinate TWIC requirements with screening programs required by other federal agencies. Another commenter requested that companies be allowed to submit amendments to their VSPs that incorporate their TWIC provisions rather than a separate addendum. The

company said this would mean less work for some companies and for the Marine Safety Center (MSC) that must do the reviews and approvals. Another commenter asked whether the TWIC Addendum would be considered SSI and whether a vessel operator could show the Addendum to people when they come on board the vessel.

One commenter recommended that the Coast Guard be required to notify an entity submitting a TWIC Addendum once the Coast Guard makes a determination of completeness. The commenter said that a confirmation letter from the Coast Guard that a complete submission has been received and is undergoing review would prevent potential delays to vessels that have not yet received an approval letter from the Coast Guard. This commenter also recommended that entities submitting a TWIC Addendum should include a contact point and method by which the Coast Guard could easily accomplish this requirement (e.g., e-mail, fax, or hard copy via surface mail).

One commenter requested that the TWIC Addendum be reviewed by the Coast Guard itself and not by outside consultants.

One commenter said that the requirement that the TWIC Addendum be kept "on site" or onboard the vessel should be revised. Specifically, the commenter said that the rule should require the TWIC Addendum to be maintained at the same location as the VSP or ASP. The commenter noted that under one approved ASP, the ASP must be maintained by the Company Security Officer at a secure location, but need not be carried on board the towing vessel. The commenter requested that the same approach be followed with the TWIC Addendum.

One commenter posed several questions regarding how this requirement would apply to OCS facilities (§ 106.115). The company asked if the requirement would apply to a foreign-flag MODU "on location" if the vessel has an approved ship security plan (SSP) as required under the ISPS Code. The company also asked how the requirement would apply to a non-self-propelled foreign flag MODU "on location" working next to or over an OCS facility that is required to comply with TWIC requirements.

Several commenters stated that Coast Guard should provide clarification on why companies and vessels need to integrate the TWIC Addendum into the ship's security plan. They said that if set up properly, the TWIC Addendum could be a stand-alone document as easy reference for persons with security

duties that are authorized to view this information.

One commenter notes that, as proposed, §§ 105.500 to 105.510 would allow an owner/operator to resubmit an entire security plan with a list of sections amended as the TWIC Addendum, but once approved, it would carry the same expiration date as it had prior to the amendment. He recommended that if the revised plan were submitted to the COPT with a revised facility security assessment, that a new time line should start and the plan should be approved for five years from the date of approval.

One commenter recommended that the TWIC Addendum requirements (33 CFR 105.120, 33 CFR 105.200 and 33 CFR 105.500–510) should be revised to explicitly require facilities to designate the secure area within which access control is required. The commenter stated that once the Coast Guard has approved the TWIC Addendum, the facility would be protected from inspectors voicing their personal opinion that the secure area does not comply with their interpretation of the definition.

We removed the TWIC Addendum requirement from the final rule when we determined that the reader requirements would be delayed until a subsequent rulemaking. The purpose of the TWIC Addendum was to allow the owner/operator to explain how the readers would be incorporated into their overall access control structure, within the standards provided in the NPRM. With the removal of the reader requirements from this final rule, we feel it is appropriate to also remove the TWIC Addendum requirement. In order to ensure that security is not compromised, we have added to the access control provisions in each part (33 CFR parts 104, 105, and 106) to provide specific security measures (as opposed to performance standards) to be implemented by owners/operators in the area of access control. Additionally, because we envision the TWIC Addendum to be a part of the subsequent rulemaking on reader requirements, we felt it would be overly burdensome to also require a TWIC Addendum at this point in time.

As the TWIC Addendum requirement is no longer included in this final rule, we will address these concerns in a subsequent rulemaking.

One commenter said that Coast Guard-approved VSPs should dictate security provisions once an individual is onboard the vessel and that the proposed rule should not establish duplicative security requirements. The commenter said that the VSPs limit

access to vessels generally and in particular prohibit access of unauthorized individuals to restricted areas of vessels. The commenter went on to state that TWICs should be used only as a basic identification device and proposed 49 CFR 1572.23 and 33 CFR 104.265 should be amended so that mariners are only subject to the existing VSPs when onboard a vessel.

We disagree that the TWIC establishes duplicative security requirements. The TWIC will enhance existing security requirements by improving the ability of owner/operators to prevent access by unauthorized individuals to restricted areas of the vessel and the vessel in general. Therefore, we decline to adopt the recommendation.

One commenter encouraged the Coast Guard to provide for some flexibility in the drafting of security plans to accommodate port workers who frequently move between secure and non-secure areas during the course of a single operation. The association said that continuous application of the limitation to gain re-entry access would be impractical and could potentially drive up costs unnecessarily. As an example, the association said that they need the ability to service cruise ship vessels without access procedures that require multiple interfacing with biometric readers.

We believe that the use of the TWIC as a visual identity badge, as required in this final rule, will alleviate some of the burden noted in this comment.

One commenter opined on the application of the TWIC requirements to shipyards involved in building and repairing U.S. military and Coast Guard vessels. The commenter stated that these shipyards must already comply with DOD security requirements, and claimed that the security afforded by the MTSA regulations is less comprehensive than the security provided by DOD security measures. The commenter said that complying with both sets of security requirements would be costly and could potentially reduce security by causing confusion and increasing administrative burdens. The commenter noted that the increased costs and administrative delays would be borne ultimately by the U.S. Navy and Coast Guard, and for these reasons requested that the shipyards be exempted from complying with the TWIC rule.

We disagree with this comment as it pertains to “all shipyards.” If a shipyard falls within the applicability of the MTSA regulations and is required to submit a FSP under 46 U.S.C. 70105, then any individual requiring unescorted access to a secure area is

required to have a TWIC. We note here that shipyards are specifically exempt from 33 CFR part 105 applicability (see 33 CFR 105.110(c)), and would only come under the facility security regulations if the shipyard is subject to a separate applicability requirement, such as being regulated under 33 CFR part 154, requirements for facilities transferring oil or hazardous material in bulk.

Both the NPRM and the final rule provide for a means through which security threat assessments done by other governmental agencies may be deemed comparable. If there are background checks in place under the DOD programs, and if those background checks include security threat assessments that are deemed comparable to the one done by TSA, then individuals may receive their TWIC at a reduced cost, but they will still need to apply at a TSA TWIC enrollment center.

Commenters stated that the rule assumes that people with TWICs will be facility employees, but that many are not (particularly truckers).

We disagree with these comments. As we stated in the NPRM, the TWIC requirements applies U.S.-credentialed mariners and to anyone seeking unescorted access to secure areas within MTSA-regulated vessels or facilities. It is not limited to facility employees, nor did we assume it would be.

One commenter noted that FSPs differ based on the threat assessment conducted for each facility. He said that the NPRM might encourage a misunderstanding among the public that every facility is “doing business” strictly according to the Code of Federal Regulations (CFR). He said, “It is very difficult sometime for people to understand that [a facility security plan] may not specifically reflect what the CFR says.”

We do not agree with this comment. If a facility is operating under its approved FSP, then it is in compliance with the regulations. The MTSA regulations are performance standards, and as such there are a variety of ways in which a facility might meet the standards contained therein. Unless a facility has been granted a waiver from portions of the regulations, we fail to see how a FSP would not reflect what is stated in the CFR.

10. Compliance Dates

The NPRM proposed requiring owners/operators to develop and submit TWIC Addendums within six months of publication of the final rule. One commenter pointed out that the Coast Guard allows itself five years to fulfill

its responsibilities, but owners/operators only get 6 months. One commenter wanted the text regarding TWIC Addendum submission to be revised to read "six months after such date that the Secretary deems the program has been fully implemented within the maritime work force ashore." One commenter wanted six months to be extended to at least one year or one year from the time the Coast Guard approves the TWIC Addendum. This would allow time for adjusting capital budgets and integrating the TWIC readers/system with existing access control systems. One commenter wanted to know what happens with regards to this timeframe if TWIC readers are not available when the implementation period begins or are not readily able to be integrated into existing systems.

These sections of the NPRM also would have required vessel, facility, and OCS facility owners/operators be operating according to their approved TWIC Addendum between 12 and 18 months after publication of the final rule, depending on whether enrollment has been completed in the port in which the vessel is operating. One commenter expressed concern that the 750,000 cards needed for initial enrollment cannot be produced within 18 months. Eight commenters believed the timeline is totally unrealistic. One commenter recommended that the "effective dates" section be reserved until it is demonstrated that the documents can be issued and equipment is both available and functional, and stated that a subsequent notice could be published in the **Federal Register** establishing effective dates of the access control and credentialing provisions when they are ready. Five commenters requested the deadline be extended. Three commenters wanted to extend the deadline specifically to afford time to budget for TWIC compliance (which typically requires a three-year lead time) and/or request/receive Federal grant funding.

The TWIC Addendum requirements have been removed from this final rule, and as such it is not necessary to respond to them at this time. We will keep them in mind as we draft our NPRM on reader requirements. As noted above, we have also revised the compliance dates slightly. Vessels will now have 20 months from the publication date of this final rule to implement the new TWIC access control provisions. Facilities will still have their compliance date tied to the completion of initial enrollment in the COTP zone where the facility is located. This date will vary, and will be announced for

each COTP zone at least 90 days in advance by a Notice published in the **Federal Register**. The latest date by which facilities can expect to be required to comply will be September 25, 2008. Additionally, mariners will not need to hold a TWIC until September 25, 2008. They may rely upon their Coast Guard-issued credential and a photo ID to gain unescorted access to secure areas to any facility that has a compliance date earlier than September 25, 2008.

One commenter stated that the final rule should clearly state the dates for compliance, and found § 104.115(d)(2) to be confusing as written. Two commenters argue that the TWIC enrollment process will never be "complete" since employers will always be submitting new applicants for enrollment, and asked who determines that enrollment is complete.

We are sensitive to these comments, however until the contract for the entity that will be operating enrollment centers is complete, we will not know exactly what date will apply to each COTP zone. We will communicate more specific dates as they become available, but can state that we expect that initial enrollment (*i.e.*, the enrollment rollout) will be complete nationally within 18 months of the first TWIC enrollment.

One commenter believed that the schedule for the applicant to provide information is confusing. The implementation schedule in § 1572.19 appears to contradict the schedule in § 104.115.

In order to reduce or eliminate any confusion, we point out that § 1572.19 applies to the individual TWIC holder and § 104.115 applies to vessel owners and operators of regulated vessels.

One commenter said the rule needs to clarify and focus on the Access Control System pilot timeline. Operational tests in selected pilot ports and terminals should be concluded and the TSA data interfaces checked and proven before the Access Control System is designed and the TWIC Addendum created. It is not clear if the timeframes apply to just the TWIC rollout or to both the TWIC and the Access Control System. Three commenters felt that the timeframe could potentially cause significant additional costs to the industry (*i.e.*, obtaining equipment and systems, hiring personnel to run the programs, etc.). Two commenters said the deadline for compliance listed in 49 CFR 1572.19 is unreasonable. It should be extended to a minimum of 18 months from the implementation of the final rule. Six commenters expressed the need for proper field testing of the biometric readers prior to usage. Two commenters

were concerned about the logistics of processing applications and issuing TWIC cards to hundreds of thousands of workers. One commenter believed TWIC is being implemented due to political issues and pressures. One commenter thought the timeline should be changed to start compliance after the technology for the cards and the readers has been proven to work instead of the date the final rule is published. Three commenters stated the rule needs clarification between page 29407, where it discusses a phased enrollment process, and page 24909, where it lists timeframes for plans and compliance. They stated that the timeframes do not allow for a phased process. All commenters recommend adopting the phased process, and one added it should be based on risk and employee access to critical infrastructure.

One commenter wanted compliance dates to begin after the Coast Guard has approved the revised plans. Another asked the Coast Guard to review their implementation timeline and ensure that industry has adequate time to successfully implement all of the requirements.

With the removal of many of the more technologically complex portions of the NPRM from this final rule, we have attempted to clarify compliance deadlines for this final rule within the regulation text. The initial enrollment period will be a phased enrollment period, which we estimate will take 18 months to complete. Owners/operators of vessels will be required to comply with the TWIC provisions of this final rule on September 25, 2008. This means that by this date, vessel owners/operators will need to begin visually inspecting TWICs before they grant individuals unescorted access to secure areas. However, many workers on vessels will be required to use a TWIC to access facilities en route to their vessel. Additionally, enrollment center scheduling has been set up to address initial enrollments of merchant mariner and non-merchant mariner workers concurrently at each port. Mariners may apply at any TWIC enrollment center, at any time during the enrollment period. Although mariners are not required to have a TWIC until the end of the enrollment period, they are encouraged to apply early. Vessel owners/operators will be better served ensuring their crews are enrolled during initial enrollment periods because they may need to access many different facilities throughout the country, and facility owner/operators must be in compliance with the access control provisions as the initial roll out enrollment in their COTP zone is completed. As noted above,

these exact dates will be announced in **Federal Register** Notices.

Two commenters requested implementation of TWIC cards be delayed for vessel personnel until the Coast Guard has redesigned its MMC to incorporate TWIC security features or at least 18 months after TWIC reader systems are ready.

With the removal of the TWIC reader requirements from this final rule, this comment is no longer relevant. However, we note that the compliance date of this final rule, for vessel owners/operators, has been changed. Vessel owners/operators need not begin checking for TWICs until 20 months after the publication date of the final rule. Workers on vessels will still be subject to the security procedures at 105 and 106 facilities. Additionally, enrollment center scheduling has been set-up to address initial enrollments concurrently with MMD and non-MMD workers at each port. Vessel personnel will be better served enrolling during initial enrollment periods at each port.

11. General Compliance Issues

One commenter wanted to know how the Coast Guard is going to ensure compliance with the TWIC program. Another cited a need for a means to verify the status of a TWIC in the field and suggested that at a minimum a call center phone number and electronic means are needed. They also suggested an investigation into the costs and benefits of equipping law enforcement personnel with the means to validate driver fingerprints against a TWIC.

At least until we are able to finalize a second rulemaking to impose reader requirements on the maritime community (as appropriate), the cards will be used for access control as visual identity badges instead of being required to be read by an owner or operator's reader at access control points. Additionally, the Coast Guard will be confirming the identity of TWIC holders using hand-held readers, uploaded with the most recent hotlist, during its already existing annual facility and vessel MTSA compliance exams, unannounced facility and vessel spot checks, and for cause as needed. Finally, although the installation of readers is not currently required, the hotlist will be made available to vessel and facility owners and operators should they voluntarily decide to use the credentials within their existing physical access control systems. As an example, an owner or operator could write to the magnetic strip on the card or read the CHUID stored on the chip embedded in the card to tie it into a

legacy system that checks the TWIC against the hotlist.

Another commenter wanted to know what protection there is if the facility that you are going to does not comply with the TWIC program.

If the facility does not comply because the MTSA regulations do not apply to it, there is no issue. If however, a MTSA-regulated facility does not visually inspect TWICs as required by this final rule, they are subject to the civil penalty provisions found in 33 CFR 101.415. Anyone who knows of such non-compliance should make a report to the National Response Center (NRC), using the contact information found in 33 CFR 101.305, as such non-compliance is a breach of security.

Two commenters are concerned that TSA and the Coast Guard want to publish a final rule before the end of the year and will not adequately address the numerous uncertainties and questions on this proposed rule that were raised by the commenters.

We disagree with this comment. We have considered each and every comment submitted to the docket during the 45-day comment period, as well as all of the comments received at the four public meetings that were held in late May and early June. We have made several changes to the proposed rule as a result of the issues and concerns raised, the biggest being the delay of the card reader and associated requirements. Additionally, in this "Discussion of comments and changes," we have responded to all of the comments we received.

Four commenters requested that the agencies issue a TWIC NVIC to assure consistent interpretation and application of the program. They also advised that TSA should develop simplified integration plans to assist companies with the implementation.

One commenter suggested that TSA and Coast Guard offer "best practices" for industry to use. As an example, the company cited the need for suggestions on handling contractor personnel during major construction projects and plant turnarounds.

We agree that a NVIC will be necessary to assist customers with compliance as well as assure consistency nation-wide; this will be forthcoming to help interpret the provisions of this rule. We are also issuing robust field guidance to all of our COTPs, to ensure uniform application of the requirements.

One commenter expressed concern that union involvement may slow the enrollment process. The commenter wanted to make sure that labor

agreements and arrangements are addressed in TWIC.

We do not feel that this final rule is the place to address labor concerns between facilities and unions.

12. Additional Requirements—Cruise Ships

Section 104.295(a)(1) proposed higher burdens on U.S. cruise ships, such as requiring that an individual's identity be checked against their TWIC at each entry to the vessel, and that the validity of the TWIC be verified with TSA at a higher rate than for other vessels. Commenters said that these additional requirements are cost-prohibitive and unfair to owners and operators of U.S.-flagged cruise ships and should be applicable to foreign cruise ships. One commenter opposed this provision, stating that this requirement is excessive, burdensome and does not respond to a demonstrated risk, and under lower MARSEC level requirements, it is not necessary to verify the identity of someone who is a known employee.

While the reader requirements have been removed from this final rule, we do not agree with the comments. Cruise ships do carry a higher risk than other passenger vessels, as the higher number of passengers on-board creates a more attractive target to terrorists. Additionally, the higher number of employees, including licensed crew, entertainers, wait staff, and other unlicensed crew, make it less likely that all employees will be "known" to the security personnel checking credentials. However, we will keep these comments in mind as we draft the NPRM to re-propose reader requirements.

Other commenters stated that most procedures for access can be covered under a vessel's security plan. One commenter said the crew was at the heart of the security plan and will ensure vessel security. One commenter suggested that instead of requiring card readers at every vessel entry point, employees should scan their cards at the facility entry point prior to boarding their assigned vessel. Another commenter stated that the proposed rule should be edited to allow for spot-checking of passengers and employee-displayed badges as mandated by a Coast Guard approved VSP at MARSEC Level 1, as current security plan specify.

These comments are no longer applicable, as the final rule does not include the requirements for readers and biometric verification. We will keep them in mind as we draft the NPRM to re-propose reader requirements.

Under proposed § 104.295(a)(2), at MARSEC Level 2, the owner or operator